DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE COPIAS DE RESPALDO EN LA EMPRESA CORVESALUD IPS BASADO EN LA NORMATIVA DE SEGURIDAD NTC-ISO-IEC 27001:2013

JOBANI CAÑON GALVIS
WILBER CALDERÓN MARIÑO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA DE SISTEMAS, CUNDINAMARCA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2017

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE COPIAS DE RESPALDO EN LA EMPRESA CORVESALUD IPS BASADO EN LA NORMATIVA DE SEGURIDAD NTC-ISO-IEC 27001:2013

JOBANI CAÑON GALVIS
WILBER CALDERÓN MARIÑO

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Directora de Proyecto
ING. LORENA OCAMPO CORREA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA DE SISTEMAS, CUNDINAMARCA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2017

Nota de aceptación

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C, 5, noviembre de 2017

Este trabajo se lo dedicamos a nuestros Padres, porque ellos siempre han estado a nuestro lado en todo momento, siempre aconsejándonos, ayudándonos y sobre todo guiándonos para seguir adelante.

También queremos dedicarlo al esfuerzo y constancia de aquellas personas que han impulsado nuestras vidas acompañándonos en los momentos difíciles.

AGRADECIMIENTOS

Agradecemos a Dios, quien nos da la fuerza necesaria para seguir adelante con nuestros proyectos, a nuestros padres por su esfuerzo, apoyo incondicional, por creer en nosotros y nuestros sueños, A nuestros familiares y amigos que aportaron su grano de arena para este nuevo logro.

A nuestras parejas por su amor incondicional, su compañía y el ánimo que nos brindaron cuando desfallecíamos.

A los ingenieros Oscar Méndez y Oscar Callejas por toda su colaboración en el desarrollo de este proyecto.

CONTENIDO

pág.

INTRODUCCIÓN 12

1. PLANTEAMIENTO DEL PROBLEMA 13
1.1 FORMULACIÓN DEL PROBLEMA 13
1.2 JUSTIFICACIÓN 13
1.3 OBJETIVOS 14
1.3.1 Objetivo General 14
1.3.2 Objetivos Específicos 14

2. MARCO REFERENCIAL 16
2.1 MARCO TEÓRICO 16
2.2 MARCO CONCEPTUAL 16
2.2.1 Gestión de seguridad de la información 16
2.2.2 Sistema de gestión de seguridad de la información 16
2.2.3 Normas ISO sobre gestión de seguridad de la información 17
2.2.4 Descripción general de Magerit 18
2.2.5 Metodología Magerit versión 3 19
2.2.6 Organización de las guías. La metodología está dividida en tres volúmenes 20
2.2.7 Proceso de gestión de riesgos 22
2.2.8 Pasos a seguir desde la metodología Magerit. 22
2.2.8.1 Tipificación de los activos 22
2.2.8.2 Amenazas 22
2.2.8.3 Salvaguardas 22
2.3 MARCO HISTÓRICO 24
2.4 MARCO LEGAL 25
2.4.1 Contexto de la organización 25
2.4.2 Estado actual 25
2.4.3 Misión de la entidad 25
2.4.4 Visión de la entidad 25
2.4.5 Actividades que desarrolla la entidad 25
2.4.6 Estructura organizacional 26
2.5 ANÁLISIS DE BRECHA DE LA ENTIDAD. 30
2.5.1 Contexto de la organización. 32
2.5.2 Liderazgo 33
4.5.3 Política 34
2.5.4 Planificación 35
2.5.5 Soporte 35
2.5.6 Operación 36
2.5.7 Evaluación del desempeño 37
2.5.8 Mejora. 38

3. DISEÑO METODOLÓGICO 39
3.1 SELECCIÓN METODOLOGÍA 39
3.2 ANÁLISIS DE RIESGOS 39
3.3 CARACTERIZACIÓN DE LOS ACTIVOS DEL SISTEMA DE COPIAS DE RESPALDO 39
3.3.1 Identificación de activos 39
3.3.2 Dependencias entre activos. 42
3.3.3 Valoración de los activos 42
3.4 CARACTERIZACIÓN DE LAS AMENAZAS 45
3.4.1 Identificación de las amenazas 52
3.4.2 Valoración de las amenazas 58

4. PLAN DE TRATAMIENTO DE RIESGOS CON BASE EN LOS CONTROLES DE LA NORMA NTC-ISO-IEC 27001:2013 76
4.1 IDENTIFICACIÓN DE LOS CONTROLES. 76
4.2 PLAN DE TRATAMIENTO DE RIESGOS 90

5. ALCANCE Y POLÍTICA DE SEGURIDAD 104
5.1 ALCANCE DE LA POLÍTICA GENERAL PARA CORVESALUD 104
5.2 POLÍTICA GENERAL DEL SGSI PARA CORVESALUD IPS 104
5.3 ALCANCE Y POLÍTICA PARA EL SERVIDOR DE COPIAS DE RESPALDO 105
5.4 POLÍTICA DEL SERVIDOR DE COPIAS DE RESPALDO 106
5.5 OBJETIVOS DE LA POLÍTICA DEL SERVIDOR DE COPIAS DE RESPALDO 106
5.6 POLÍTICAS GENERALES 107
5.7 POLÍTICAS ORGANIZACIONALES 108
5.8 POLÍTICAS DE RECURSOS HUMANOS 108
5.9 POLÍTICAS DE GESTION DE ACTIVOS 109
5.10 POLÍTICAS DE GESTIÓN DE ACCESO DE USUARIOS 109
5.11 POLÍTICA DE CRIPTOGRAFÍA 110
5.12 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO 110
5.13 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES 110
5.14 POLÍTICAS SOBRE LA SEGURIDAD EN LAS COMUNICACIONES 111
5.15 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 111
5.16 POLÍTICAS DE LAS RELACIONES CON LOS PROVEEDORES 112

6. PLAN DE IMPLEMENTACIÓN 113

7. PLAN DE CONCIENCIACIÓN 115

8. CONCLUSIONES 117

9. RECOMENDACIONES 118

BIBLIOGRAFÍA 119

ANEXOS 122

LISTA DE CUADROS

pág.

Cuadro 1. Normas ISO 27000 18
Cuadro 2. Inventario de activos de información 40
Cuadro 3. Criterios de valoración 43
Cuadro 4. Valoración de activos 43
Cuadro 5. Catálogo de Amenazas 45
Cuadro 6. Identificación de amenazas 52
Cuadro 7. Degradación de valor y la probabilidad de ocurrencia 59
Cuadro 8. Valoración de amenazas por activo 59
Cuadro 9. Calculo del riesgo 65
Cuadro 10. Mapa de calor de riesgo = Impacto * Probabilidad 65
Cuadro 11. Evaluación de riesgos 65
Cuadro 12. Rango de valores del riesgo 73
Cuadro 13. Criticidad de los activos. 73
Cuadro 14. Riesgos a trabajar 74
Cuadro 15. Identificación de controles 77
Cuadro 16. Plan de tratamiento de los riesgos 91

LISTA DE FIGURAS

pág.

Figura 1. ISO 31000 - Marco de trabajo para la gestión de riesgos 19
Figura 2. Actividades Formalizadas 22
Figura 3. Estructura organizacional 26
Figura 4. Mapa de Procesos 27
Figura 5. Análisis de brecha de la entidad. 31
Figura 6. Contexto de la organización 32
Figura 7. Liderazgo y compromiso 33
Figura 8. Política 34
Figura 9. Planificación 35
Figura 10. Soporte 35
Figura 11. Operación 36
Figura 12. Evaluación del desempeño 37
Figura 13. Mejora 38
Figura 14 . Mapa de dependencias entre activos 42
Figura 15. Distribución del riesgo 72

LISTA DE ANEXOS

pág.

Anexo 1. Cuestionario analisis de brecha de la entidad 122

INTRODUCCIÓN

La mayoría de las entidades de salud en general manejan información de carácter importante para los usuarios y el personal adscrito a la entidad, la cual cobra vida en los distintos procesos que se manejan. Esta información al contener los datos relevantes de la organización se convierte en un activo primordial y el cual requiere un trato especial por parte de la entidad, en el caso de la salud se observa cómo las historias clínicas de los pacientes se pierden, las cuales son importantes en su diario vivir y en especial si se lleva algún proceso clínico. Desde el ámbito empresarial se observa como todas las áreas de trabajo pueden padecer pérdida de información de tipo administrativa, contable y del personal. De ahí surge la necesidad de que esta información siempre esté disponible en las mejores condiciones, para que el usuario o los mismos empleados puedan acceder a ella de manera inmediata y realizar sus procesos.

El diseño de políticas, metodologías, procesos, controles y técnicas o normas de seguridad de la información que propendan por mejorar estos procesos y proteger los activos de información, harán que la empresa Corvesalud IPS cobre un mayor valor ante sus clientes, junto con una mejora en los procesos del manejo propio de la entidad.

Por esta razón se requiere diseñar un sistema de gestión de seguridad de la información para el proceso de copias de respaldo basado en la norma ISO 27001 -2013 para realizar el análisis, evaluación, plan de tratamiento de los riesgos y planteamiento de políticas, que sean una propuesta de cómo funcionaría el sistema de gestión de seguridad de la información en el proceso de copias de respaldo.

1. PLANTEAMIENTO DEL PROBLEMA

La empresa Corvesalud IPS no cuenta con un sistema de seguridad de la información, ni ningún departamento especializado en la misma, lo que dificulta tener una visión global y trasversal de su seguridad, en cuanto a las personas, procesos y tecnologías. Esto hace que se dificulte gestionar los riesgos del proceso de copias de respaldo, por tal motivo no hay una participación activa de la organización en la definición de procedimientos, planeación y uso de controles, basados en la en la evaluación de riesgos.

La organización tiene la necesidad de asegurar sus activos de información en especial el proceso de copias de respaldo, para mantener la información disponible y protegida contra cualquier evento que pueda afectar la continuidad del negocio, de ahí la importancia del diseño de una política de seguridad de la información, de la identificación, valoración y tratamiento de los posibles riesgos de la seguridad de la misma.

1.1 FORMULACIÓN DEL PROBLEMA

¿De qué manera se puede orientar la protección en los activos de información del proceso de copias de respaldo de la empresa Corvesalud IPS?

1.2 JUSTIFICACIÓN

La entidad Corvesalud IPS necesita tener un proceso de gestión de seguridad de la información, en el que se realice un detallado análisis de riesgos y diseño de controles enfocados en al proceso de copias de respaldo. Con este ejercicio se pueden alcanzar diversos objetivos que aportarían valores a la entidad tales como una mejora de la imagen corporativa, el cumplimiento legal, reglamentario, la protección y continuidad del negocio. El diseño del sistema de gestión de seguridad de la información para el proceso de copias respaldo de la información basado en la norma ISO 27001, permitirá a Corvesalud IPS estructurar las bases necesarias para un adecuado modelo de seguridad de la información en la empresa, lo que puede propiciar la continua mejora, la debida permanencia y evolución a través del tiempo.

Un sistema de gestión de seguridad de la información, le permite a la empresa gestionar de manera efectiva los riesgos asociados a la seguridad de la información mediante la identificación de amenazas que puedan llegar a comprometer la integridad, disponibilidad y confidencialidad de sus activos de información y con esto poder establecer mecanismos para minimizar el impacto en caso de presentarse la materialización de un riesgo. El diseño de un sistema de gestión de seguridad de la información para el proceso de copias de respaldo en la empresa Corvesalud IPS va de la mano con distintos procesos internos, los

cuales generarían mayor confianza y eficacia al momento de manipular información, esto impactaría de manera positiva y rentable para la empresa.

Todo personal en una organización debe tener sentido de pertenencia y apropiación en temas de seguridad en cada uno de los procesos de la entidad, teniendo una participación activa en la planeación, definición, identificación e implementación de controles y medidas orientadas a velar por la seguridad de la información de la organización.

Este proyecto pretende despertar la conciencia de los funcionarios de la entidad, con relación a los riesgos que pueden afectar la seguridad de la información no solo evitando perdida de la misma, sino cualquier evento que pueda afectar el proceso de la información. Por último, promover que sean los funcionarios los que adopten, interioricen, acaten las políticas, procedimientos y prácticas de seguridad definidas en la empresa, a su vez comprendan las implicaciones, peligros y riesgos de sus acciones.

En Colombia la norma NTC ISO/IEC 27001:2013 estandariza y describe cómo gestionar el sistema de gestión de seguridad de la información, buscando mejorar con ello el proceso de copias de respaldo de la entidad, por lo cual estará dando cumplimiento a lo exigido por la ley.

1.3 OBJETIVOS

1.3.1 Objetivo General. Diseñar un sistema de gestión de seguridad de la información para el proceso de copias de respaldo en la empresa CORVESALUD IPS, basado en la normativa de seguridad NTC-ISO-IEC 27001:2013

1.3.2 Objetivos Específicos

- Identificar la situación actual de la empresa, con relación a la gestión de seguridad de la información en el proceso de copias de respaldo.

- Realizar la descripción de los activos de la entidad en el proceso de copias de respaldo.

- Realizar el análisis de riesgos con base en la metodología Magerit versión 3.

- Diseñar políticas de seguridad de la información, para el proceso de copias de respaldo con base en la norma NTC-ISO-IEC 27001:2013.

- Establecer un plan de implementación del Sistema de Gestión de la información para el proceso de copias de respaldo en la empresa CORVESALUD IPS.

- Diseñar el plan de tratamiento de los riesgos, con base en los controles de la norma NTC-ISO-IEC 27001:2013.

- Diseñar plan de concienciación para los funcionarios, proveedores, terceros y usuarios de CORVESALUD IPS.

2. MARCO REFERENCIAL

2.1 MARCO TEÓRICO

El proyecto se va a desarrollar en la IPS Corvesalud en la cual se percibe la necesidad de diseñar un sistema de gestión de seguridad de la información para el proceso de copias de respaldo, con el fin de proponer alternativas que puedan garantizar la protección de la información de los usuarios, puesto que en la actualidad la empresa carece de algunos componentes tecnológicos que permitan manejar de manera adecuada la seguridad de la información. Cabe denotar que el proceso con que la IPS viene manejando su información se basa en métodos tradicionales de almacenamiento como lo son CD/DVD, Unidades externas de guardado y copias de seguridad en el mismo equipo usando particiones en el disco duro interno, lo que puede generar una pérdida de esta misma en cualquier momento por daños en los equipos. Para lograr implementar este proyecto se debe tener en cuenta conceptos como gestión de la información y otros relacionados con la seguridad de la información.

2.2 MARCO CONCEPTUAL

A continuación, se presentan algunas definiciones importantes relacionadas con el sistema de gestión de seguridad de la información que se busca diseñar, así como las principales características de la metodología a utilizar, para este caso MAGERIT.

2.2.1 Gestión de seguridad de la información. Es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías[1] .

2.2.2 Sistema de gestión de seguridad de la información. Para que las organizaciones puedan desarrollar de manera correcta su gestión de seguridad de la información, es necesario contar con un proceso sistemático, documentado, conocido y adoptado por toda la organización, basado en un enfoque de gestión de riesgos, que brinde confianza a las partes interesadas acerca de la manera adecuada de gestionar los riesgos.

[1] ISO-IEC 27000: 2014. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario. [En Línea]: [Citado 13, junio 2017]. Disponible en internet: <URL: <https://www.normasiso.net/wp-content/uploads/2016/10/iso-27000.pdf>

De acuerdo a la norma NTC-ISO-IEC 27001:2013[2], un sistema de gestión de seguridad de la información tiene por finalidad preservar la confidencialidad, integridad y disponibilidad de la información, a través de la aplicación de un proceso de gestión del riesgo.

2.2.3 Normas ISO sobre gestión de seguridad de la información. Una norma es un documento de uso voluntario y es producto del consenso de las partes interesadas y que deben aprobarse por un organismo de normalización reconocido.

El ISO (International Organization for Standardization, Organización Internacional para la Estandarización) es un organismo internacional que se dedica a desarrollar reglas de normalización en diferentes ámbitos, entre ellos la informática. El IEC (International Ellectrotechnical Commision) es otro organismo que publica normas de estandarización en el campo de la electrónica.

ISO 27000. La serie de normas ISO/IEC 27000 se denominan requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI), estas normas proporcionan un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre las siguientes materias:

- Sistema de gestión de la seguridad de la información
- Valoración de riesgos
- Controles

En la serie de normas ISO 27000 los rangos de numeración reservados por ISO van del 27000 al 27019 y del 27030 al 27040. El cuadro 1, Serie de normas ISO 27000, presenta una descripción de los estándares más destacados de la serie Gestión de seguridad de la información.

[2] Ibíd. Requisitos. Capítulo Introducción. P. i.

Cuadro 1. Normas ISO 27000

Norma	Alcance
ISO 27000	Contiene una visión general de las normas de la serie y un conjunto de definiciones y términos que serán usados en la serie
ISO 27001	Que sustituye a la ISO 17799-1, abarca un conjunto de normas relacionadas con la seguridad informática. Se basa en la norma BS 7799-2 de British Estándar, otro organismo de normalización. Según esta norma, que es la principal de la serie, la seguridad de la información es la prevención de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento.
ISO 27002	Que se corresponde con la ISO 17799, y que describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendados relacionados con la seguridad.
ISO 27003	Que contiene una guía para la implementación de la norma.
ISO 27004	Que contiene los estándares en materia de seguridad para poder evaluar el sistema de gestión de la seguridad de la información.
ISO 27005	Que recoge el estándar para la gestión del riesgo de la seguridad.
ISO 27006	Requisitos a cumplir por las organizaciones encargadas de emitir certificaciones ISO 27001.
ISO 27007	Suministra una guía para las entidades acreditadas de certificación para auditar SGSI.

Fuente: Los Autores

2.2.4 Descripción general de Magerit. Es el acrónimo de “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas”, elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

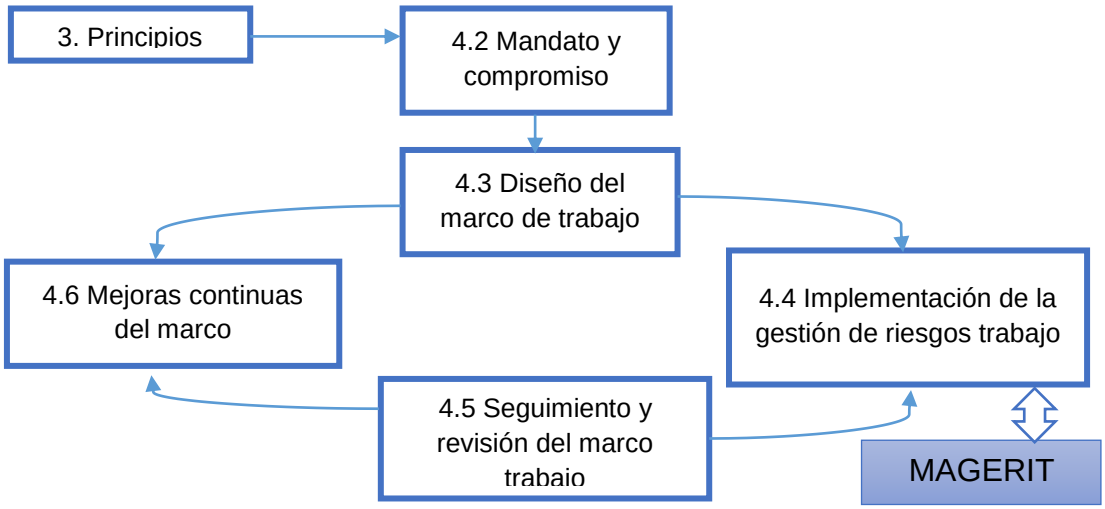
La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT propone dos grandes tareas en la *gestión del riesgo*, la primera es el *análisis de riesgos*, los cuales permiten determinar qué tiene la organización y valorar lo que podría pasar, y la segunda es el *tratamiento de los riesgos*, que propende una defensa a conciencia con el fin de evitar que pase algo perjudicial

para el sistema y preparándose para actuar en el menor tiempo posible ante algún evento; esto con el fin de sobrevivir a los incidentes que se presenten y seguir operando en las mejores condiciones.

2.2.5 Metodología Magerit versión 3. Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.[3] En la figura 1, ISO 31000 - Marco de trabajo para la gestión de riesgos. Se muestran las tareas del proceso de gestión del riesgo.

Figura 1. ISO 31000 - Marco de trabajo para la gestión de riesgos



Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, Magerit – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, 2012, p. 7.

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es

[3] Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, Magerit – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, 2012, p. 7.

riguroso, las conclusiones serán de poco fiar. Es por ello que en Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.[4]

2.2.6 Organización de las guías. La metodología está dividida en tres volúmenes:

- Volumen I: Método
- Volumen II: Catalogo de Elementos
- Volumen III: Guía de Técnicas

Volumen I: Método. Esta guía describe la estructura que debe tener el modelo de gestión de riesgos y estructurada de la siguiente forma:

Capítulo I: Esta sección relata por qué fue desarrollada esta metodología, así como los organismos que intervinieron en su creación y algunos conceptos generales.

Capitulo II Visión de Conjunto: Presenta dos grandes tareas que se deben realizar, específicamente las actividades de análisis y tratamiento de riesgos para tener un proceso integral de gestión de riesgos.

Capitulo III Método de Análisis de Riesgos: En este apartado se explica en detalle cada uno de los pasos que se realizan en el análisis de los riesgos y así poder determinarlos.

Capítulo IV Proceso de Gestión de Riesgos: Describe todas las actividades que se hacen dentro de la Gestión de Riesgos.

Capítulo V Proyectos de Análisis de Riesgos: Presenta las consideraciones necesarias para que las actividades dentro del proyecto de análisis de riesgos lleguen a buen fin, ya sea con un auditor externo o interno.

Capítulo VI Plan de Seguridad: Comprende todas las actividades para llevar a cabo planes de seguridad, para materializar las decisiones adoptadas en el tratamiento de riesgos.

Capítulo VII Desarrollo de Sistemas de Información: Está basado en la seguridad de los sistemas de información teniendo en cuenta varios puntos de vista para mitigar el riesgo.

Capítulo VIII Consejos Prácticos: Presenta una serie de comentarios que sirven de guía en el diseño de análisis de riesgos.

[4] Ibíd., p. 8

Volumen II: Catalogo de Elementos. Es un inventario que puede utilizar la entidad con el fin de enfocarse en el análisis de riesgos, contiene una división de los activos de información que deben valorarse, las características de los mismos y un listado de amenazas y controles para tener en cuenta; tiene como objetivos:

- "Facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis"[5].

- Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos[6].

Volumen III: Guía de Técnicas. Describe las diferentes técnicas utilizadas en análisis y gestión del riesgo. Se considera técnica a un conjunto de heurísticos y procedimientos que ayudan a alcanzar los objetivos propuestos.

Para cada una de las técnicas referenciadas:

- Se explica brevemente el objetivo que se persigue al utilizarlas.
- Se describen los elementos básicos asociados.
- Se exponen los principios fundamentales de elaboración.
- Se presenta una notación textual y/o gráfica y
- Y se citan las fuentes bibliográficas que, sin ser exhaustivas, se han estimado de interés para que el lector profundice en cada materia[7].

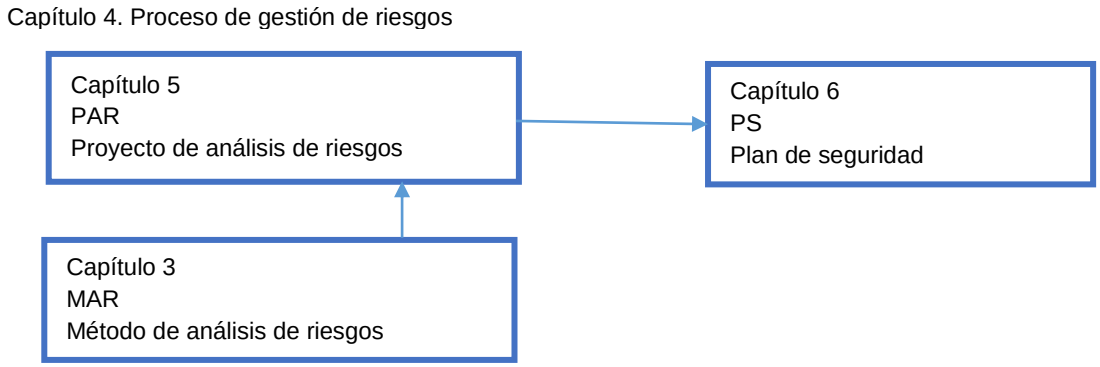
Las guías que expone son:

- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Análisis coste-beneficio
- Diagramas de flujo de datos (DFD)
- Diagramas de procesos
- Técnicas gráficas
- Planificación de proyectos
- Sesiones de trabajo: entrevistas, reuniones y presentaciones
- Valoración Delphi.

[5] Ibíd., p. 13.
[6] Ibíd.
[7] Ibíd., p. 4.

2.2.7 Proceso de gestión de riesgos. Tiene como objetivo identificar y tratar de manera urgente los riesgos críticos, actuando progresivamente sobre los riesgos de menor criticidad. En la figura 2, actividades formalizadas se muestra los procesos de gestión de los riesgos.

Figura 2. Actividades Formalizadas



Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, Magerit – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, 2012, p. 13.

2.2.8 Pasos a seguir desde la metodología Magerit

2.2.8.1 Tipificación de los activos. Es la información documental de los activos de la entidad con un criterio de identificación de las amenazas potenciales. Estos activos son valorados de acuerdo a las características o atributos que hacen valioso el activo, llamadas dimensiones, estas permiten valorar las consecuencias de la materialización de una amenaza y esta valoración es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Las dimensiones utilizadas en la valoración de activos son las siguientes: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Después son evaluados en una escala de valores.

2.2.8.2 Amenazas. Son todas aquellas situaciones que desencadenan en un incidente dentro de una organización, realizando un daño material o pérdidas inmateriales de los activos de información. Como ya se ha dicho anteriormente Magerit contiene un catálogo de amenazas posibles sobre los activos de un sistema información, categorizados como: desastres naturales, de origen industrial, errores y fallos no intencionados, ataques intencionados y correlación de errores y ataques.

2.2.8.3 Salvaguardas. Permiten hacer frente a las amenazas. Las de origen técnico varían con el avance tecnológico.

- Porque aparecen tecnologías nuevas,
- Porque van desapareciendo tecnologías antiguas,
- Porque cambian los [tipos de] activos a considerar,
- Porque evolucionan las posibilidades de los atacantes o
- Porque evoluciona el catálogo de salvaguardas disponibles.

En consecuencia, este catálogo de salvaguardas no entra en la selección de paquetes o productos a instalar, limitándose a establecer un paraguas taxonómico para ordenar y clasificar las diferentes concreciones materiales, tecnológicas, organizativas y procedimentales que sean de aplicación en cada momento[8].

2.3 MARCO HISTÓRICO

Corvesalud S.A.S, fue constituida mediante acta del 00655921 del 18 de julio de 1995, bajo la razón social de Corvesalud Ltda., modificada mediante acta número 40 de la junta de socios el 15 de abril de 2015, inscrita bajo número 01938763 del libro IX de la cámara de comercio de Bogotá, la cual hace referencia al cambio de nombre por Corvesalud S.A.S, cuyo objeto social, en términos generales es prestar directamente o por intermedio de personas contratadas todos los servicios de salud en las distintas ramas de medicina, así como en las especialidades médicas que su capacidad técnica y científica le permita, de conformidad con las normas legales que rigen la actividad de las instituciones prestadoras de servicios de salud, a los afiliados y beneficiarios del sistema general de seguridad social en salud dispuesto por la ley 100 de 1993 y al público en general.

Realiza labores de promoción de salud en los campos de la educación, información y fomento de la misma, así como de la prevención de enfermedades, la de recuperación y rehabilitación médica.

Igualmente comercializa todo tipo de medicamentos para la salud, elementos quirúrgicos, hospitalarios, equipos y demás bienes requeridos por los servicios de salud, así como los destinados a las labores de rehabilitación o adaptación médica.

En la actualidad consta de una sede administrativa y seis sedes de atención al usuario para servicios de salud de primer nivel en la ciudad de Bogotá y municipios aledaños como: Facatativá, Mosquera y Madrid. En cada sede se cuenta con servicios de Medicina General y Odontología, funciones administrativas, farmacias, procedimientos, línea de frente y labores de enfermería. Dichas sedes manejan gran cantidad de información, siendo como

[8] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, En: Libro II-Catálogo De Elementos. Madrid: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de Análisis de Riegos, 2012. p. 53.

dato principal, las historias clínicas de los usuarios que día a día acuden a su servicio médico. Por otra parte, toda la documentación administrativa de suma importancia que almacena cada sede en relación a medicamentos, elementos quirúrgicos, hospitalarios, equipos, pagos, procesos, directrices, archivos (texto, audio, imágenes) entre otros.

2.4 MARCO LEGAL

2.4.1 Contexto de la organización. La norma ISO/IEC 27001:2013 enmarca la importancia de conocer y comprender, los distintos factores externos e internos de la entidad, que pueden afectar o ser afectados de manera positiva o negativa por el establecimiento del Sistema de Gestión de Seguridad de la Información. Para evaluar estos contextos la norma ISO/IEC 27001:2013, incluye el capítulo "4. Contexto de la organización", donde se establece que la entidad debe determinar las situaciones y factores externos e internos que la rodean y que son pertinentes para establecer al Sistema de Gestión de Seguridad de la Información.

2.4.2 Estado actual. Corvesalud IPS es una entidad privada, organizada para la prestación de los servicios de salud a los afiliados del sistema general de seguridad social en salud, dentro de una entidad promotora de salud (Cafesalud EPS). Tiene como principio básico la calidad y la eficiencia, cuenta con autonomía administrativa, técnica y financiera, y debe propender por la libre concurrencia de sus acciones. Además de esto, Corvesalud IPS ofrece una gran variedad de prestaciones médicas, servicios y beneficios, orientados a la población con menos recursos y al público general.

2.4.3 Misión de la entidad. Corvesalud IPS presta servicios de salud a través de un modelo de atención con énfasis en una cultura de trato digno, seguridad del paciente, innovación y sostenibilidad para contribuir al bienestar de nuestros pacientes, sus familias y la comunidad[9].

2.4.4 Visión de la entidad. Gestionar los servicios de salud con altos estándares de calidad[10].

2.4.5 Actividades que desarrolla la entidad. El enfoque principal de Corvesalud IPS es la atención primaria en servicios de salud a los usuarios de la EPS Cafesalud con los siguientes servicios: medicina, odontología, enfermería y promoción y prevención.

[9] CORVESALUD IPS. ¿Quiénes Somos? [En Línea] Bogotá, D.C.: [Citado 8, julio 2017]. Disponible en internet: <URL: http://www.corvesalud.com.co/quienes-somos/>

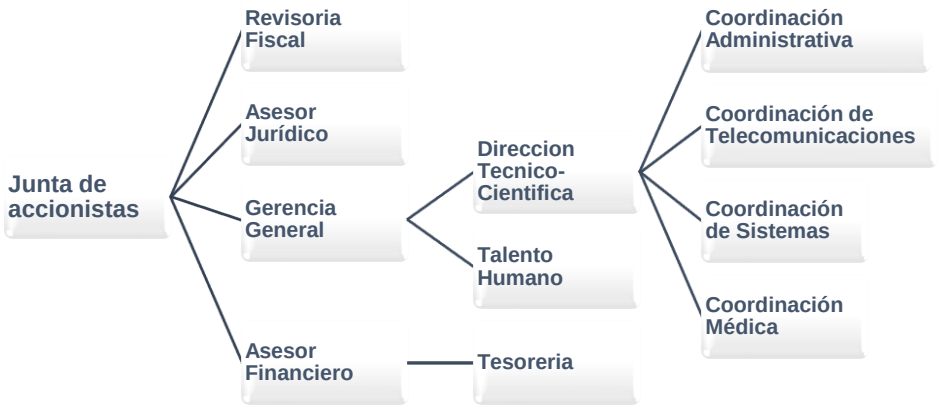
[10] CORVESALUD IPS. ¿Quiénes Somos? [En Línea] Bogotá, D.C.: [Citado 8, julio 2017]. Disponible en internet: <URL: http://www.corvesalud.com.co/quienes-somos/>

Actividades:

- Consulta externa (Medicina general).
- Vacunación.
- Procedimientos menores.
- Laboratorio y ayudas diagnósticas.
- Servicio de farmacia.
- Enfermería (Promoción y prevención, atención a maternas, crecimiento y desarrollo, citologías y atención a usuarios crónicos).
- Interconsultas (Medicina interna, medicina familiar, ginecología, pediatría, trabajo social y psicología).
- Consulta odontológica (Endodoncia, odontopediatria, higiene oral y cirugía oral).

2.4.6 Estructura organizacional. La entidad cuenta con una estructura compuesta por la junta de accionistas, revisor fiscal, asesor jurídico, gerencia general, asesor financiero, tesorería, talento humano, dirección técnico científica, coordinación de telecomunicaciones, administrativa, de sistemas y medica; estas estructuras están organizadas en el organigrama de la figura 3, estructura organizacional.

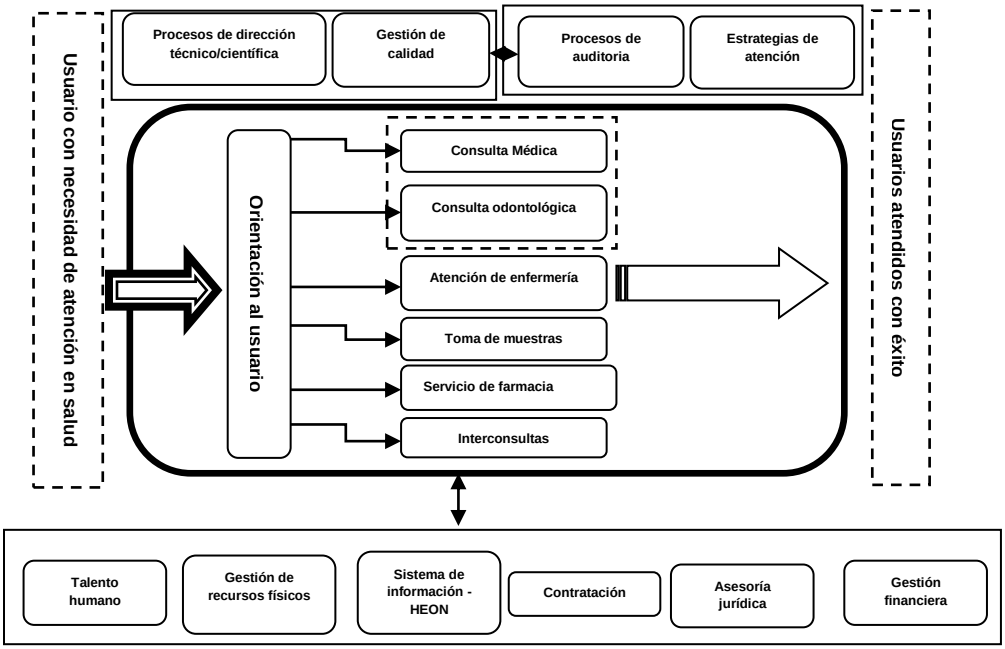
Figura 3. Estructura organizacional



Fuente: Los Autores

Además, los procesos que se generan dentro de la entidad están diagramados en la figura 4, mapa de procesos.

Figura 4. Mapa de Procesos



Fuente: Los Autores

Áreas críticas de la entidad. El área crítica de la entidad en cuanto a un proceso de copias de respaldo se refiere, incluye la parte administrativa, tesorería, contabilidad, talento humano, coordinaciones médicas y demás áreas administrativas las cuales tienen un gran flujo de información por conservar y proteger de daños y pérdidas.

Normatividad de seguridad aplicable a la entidad. Corvesalud IPS al ser una entidad prestadora de servicios de salud está vigilada y controlada por diversas entidades como: ministerio de salud, superintendencia nacional de salud, así mismo por diferentes entes de control; en base a estas organizaciones se establecen unas resoluciones y normas, por las cuales se debe regir la entidad y hacer cumplir de la manera adecuada.

Ley 100 de 1993: El sistema de seguridad social integral es el conjunto de instituciones, normas y procedimientos, de que disponen la persona y la comunidad para gozar de una calidad de vida, mediante el cumplimiento progresivo de los planes y programas que el Estado y la sociedad desarrollen para proporcionar la cobertura integral de las contingencias, especialmente las que menoscaban la salud y la capacidad económica, de los habitantes del territorio

nacional, con el fin de lograr el bienestar individual y la integración de la comunidad[11].

Artículo. 1º- Sistema de seguridad social integral. El sistema de seguridad social integral tiene por objeto garantizar los derechos irrenunciables de la persona y la comunidad para obtener la calidad de vida acorde con la dignidad humana, mediante la protección de las contingencias que la afecten. El sistema comprende las obligaciones del Estado y la sociedad, las instituciones y los recursos destinados a garantizar la cobertura de las prestaciones de carácter económico, de salud y servicios complementarios, materia de esta ley, u otras que se incorporen normativamente en el futuro[12].

Resolución 2003 de 2014: La Resolución 2003 de 2014 del Ministerio de Salud y Protección Social define los procedimientos y condiciones de inscripción de los Prestadores de Servicios de Salud y de habilitación de servicios de salud. Así mismo, adopta el Manual de Inscripción de Prestadores y Habilitación de Servicios de Salud[13].

Ley 1438 de 2011: Esta ley tiene como objeto el fortalecimiento del Sistema General de Seguridad Social en Salud, a través de un modelo de prestación del servicio público en salud que en el marco de la estrategia de atención primaria en salud permita la acción coordinada del Estado, las instituciones y la sociedad para el mejoramiento de la salud; la creación de un ambiente sano y saludable, que brinde servicios de mayor calidad, incluyente y equitativo en donde el centro y el objetivo de todos los esfuerzos sean los residentes en el país.

"Se incluyen prácticas para establecer la unificación del plan de beneficios para todos los residentes, la universalidad del aseguramiento y la garantía de portabilidad o prestación de los beneficios en cualquier lugar del país, en un marco de sostenibilidad financiera"[14].

Resolución 4107 de 2011: Esta resolución tiene por objeto reglamentar el procedimiento, los criterios, condiciones y plazos para la compra directa de cartera a las Instituciones Prestadoras de Servicios de Salud, con cargos a los recursos de la Subcuenta de Garantías del Fondo de Solidaridad y Garantía – FOSYGA y su posterior pago por parte de las Entidades Promotoras de Salud de los

[11] LEY 100 DE 1993. "Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones" Preámbulo.
[12] Ibíd. Artículo 1.
[13] MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. RESOLUCIÓN NÚMERO 00002003 DE 2014. "Por la cual se definen los procedimientos y condiciones de inscripción de los Prestadores de Servicios de Salud y de habilitación de servicios de salud"
[14] LEY 1438 DEL 19 DE ENERO DE 2011 SENADO. "Por medio de la cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones". Artículo 1.

Regímenes Contributivo y Subsidiado y las Cajas de Compensación Familiar que administren este último régimen.

*Decreto 1011 de 2006: artículo 1.- campo de aplica*ción. Las disposiciones del presente decreto se aplicarán a los Prestadores de Servicios de Salud, las Entidades Promotoras de Salud, las Administradoras del Régimen Subsidiado, las Entidades Adaptadas, las Empresas de Medicina Prepagada y a las Entidades Departamentales, Distritales y Municipales de Salud. Así mismo, a los prestadores de servicios de salud que operen exclusivamente en cualquiera de los regímenes de excepción contemplados en el artículo 279 de la Ley 100 de 1993 y la Ley 647 de 2001, se les aplicarán de manera obligatoria las disposiciones del Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud -SOGCS- de que trata este decreto, excepto a las Instituciones del Sistema de Salud pertenecientes a las Fuerzas Militares y a la Policía Nacional, las cuales podrán acogerse de manera voluntaria al SOGCS y de manera obligatoria, cuando quieran ofrecer la prestación de servicios de salud a Empresas Administradoras de Planes de Beneficios -EAPB-, Instituciones Prestadoras de Servicios de Salud -IPS-, o con Entidades Territoriales[15].

Circular 052 de 2007, por medio de la cual la Superintendencia Financiera de Colombia "establece los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios"[16], entre otros establece que las entidades vigiladas deben gestionar la seguridad de la información para lo cual pueden tomar como el estándar de las normas ISO 2700158[17].

Circular 038 de 2009, por medio de la cual la Superintendencia Financiera de Colombia determina que las entidades vigiladas deben contar con sistemas que garanticen que la información cumpla con los criterios de seguridad relacionados con la confidencialidad, integridad y disponibilidad[18] .

Ley estatutaria 1266 de 2008 "Habeas Data", que regula el manejo de la información de las personas recopiladas y almacenadas en bases de datos de terceros, en especial la información de carácter financiero, crediticio, comercial, de servicios y la proveniente de terceros países.

[15] MINISTERIO DE LA PROTECCION SOCIAL.DECRETO NÚMERO 1011 DE 2006. "Por el cual se establece el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud". Campo de aplicación.
[16] Superintendencia Financiera de Colombia, Circular externa 052 de 2007.
[17] Ibíd. numeral 3.1.2
[18] Superintendencia Financiera de Colombia, Circular externa 038 de 2009, numeral 7.5.4.1

Ley 1581 de 2012[19] que fue regulada en el Derecho 1377 de 2013[20], que definen el marco jurídico orientado a garantizar que la debida, recolección, almacenamiento, tratamiento, uso y distribución de los datos personales de los titulares por parte de terceros.

Partes interesadas de la entidad. Las partes interesadas en el diseño del sistema de gestión de seguridad para el proceso de copias de respaldo son aquellas con perfil administrativo dentro de la entidad, aquellas cuya información es fundamental y prioritaria al momento de darle un uso, estas partes administrativas hacen referencia a dependencias como: Gerencia, tesorería, talento humano, departamento de sistemas y tecnología, contabilidad y coordinaciones médicas. Los puestos de trabajo de los profesionales (Médicos, odontólogos, especialistas) no disponen de un manejo de información específico ya que se limitan a ingresar sus datos y los del usuario a la respectiva Historia Clínica almacenada de manera sistemática en los servidores de Cafesalud por medio del Sistema de Información HEON.

Por otra parte, existen dependencias asistenciales como vacunación y farmacia las cuales almacenan información de suma importancia para ser presentada ante los entes de control de salud. De esta manera son varias las partes interesadas en este proceso de seguridad en las copias de respaldo.

2.5 ANÁLISIS DE BRECHA DE LA ENTIDAD

El análisis de brecha permite identificar, el nivel de complejidad que le puede significar a la entidad implementar un sistema de la seguridad de la información. Para lo cual, se toma como referencia el análisis de brecha de la ISO 27001, el cual permite tener una visión del estado inicial o que hace falta para alcanzar el nivel de implementación adecuado, evaluando el contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño, mejora, políticas de seguridad, organización de la seguridad, seguridad relativa a los recursos humanos, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, seguridad de las operaciones, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento de sistemas de información, relación con proveedores, gestión de incidentes de seguridad de la información, aspectos de seguridad de la información para la gestión de la continuidad del negocio y cumplimiento[21].

[19] LEY ESTATUTARIA 1581 DEL 17 DE OCTUBRE DE 2012 “Por el cual se dictan disposiciones generales para la protección de los datos personales”.
[20] DECRETO 1377 DE 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.
[21] ADVISERA EXPERT SOLUTIONS LTD. Herramienta gratuita de análisis de brecha para ISO 27001 [En Línea]: [Citado 24, junio 2017]. Disponible en internet: <URL: https://advisera.com/27001academy/es/herramientas/herramienta-gratuita-analisis-de-brecha-para-iso-27001/

Para establecer el análisis de brecha de la entidad se utilizó el formato relacionado en el *Anexo A* del presente trabajo de grado. En la figura 5, análisis de brecha. Se muestran los porcentajes arrojados por las encuestas con respecto a la situación actual de la entidad. Esta encuesta fue aplicada al personal que tiene relación con el servidor de copias de respaldo, de acuerdo a la información suministrada por la entidad y la respectiva valoración de la existencia o no, del control dentro de la organización, permitiendo tener una visión del estado actual de la entidad.

Figura 5. Análisis de brecha de la entidad.

Fuente: Los Autores

En referencia al análisis de brecha realizado a las personas encargadas de la parte de tecnología de la empresa, a través de una encuesta, se puede concluir que el estado actual de la empresa en cuanto a la seguridad de la información no es óptimo, generando un 61% de anormalidad en los procesos que conllevan la seguridad de la información y un 39 % de normalidad en otros procesos. Lo anterior concluye que se deben mejorar los procedimientos para establecer mayor control sobre la información que se maneja en la empresa.

Esta encuesta fue desarrollada en el área de tecnología de la empresa, fueron encuestadas 10 personas y con base a esto, se realizó el análisis, dejando como resultado la figura 5.

2.5.1 Contexto de la organización

Figura 6. Contexto de la organización

Fuente. Los Autores

En la figura 6, contexto de la organización se observa en general, que ella no gestiona de la mejor manera ya que se muestra un 70% de no cumplimiento y se recomienda lo siguiente para realizar mejoras en este proceso:

- Garantizar el cumplimiento de las obligaciones legales para mejorar la capacidad operativa de la empresa.
- Se tiene claro cuáles son las cuestiones internas y externas que influyen en el propósito del negocio y que son relevantes para la seguridad de la información.
- Están definidas las partes interesadas de la empresa que son relevantes en la seguridad de la información (Empleados, proveedores, entre otros).
- No existe una lista de necesidades y expectativas que puedan ser evaluadas de manera cuantitativa o cualitativa en la empresa.

2.5.2 Liderazgo

Figura 7. Liderazgo y compromiso

Fuente: Los Autores

En la figura 7, liderazgo y compromiso, existe un 60 % de cumplimiento para el liderazgo en los procesos de información en la empresa y un 40% de no cumplimiento, debido a estos resultados se define lo siguiente:

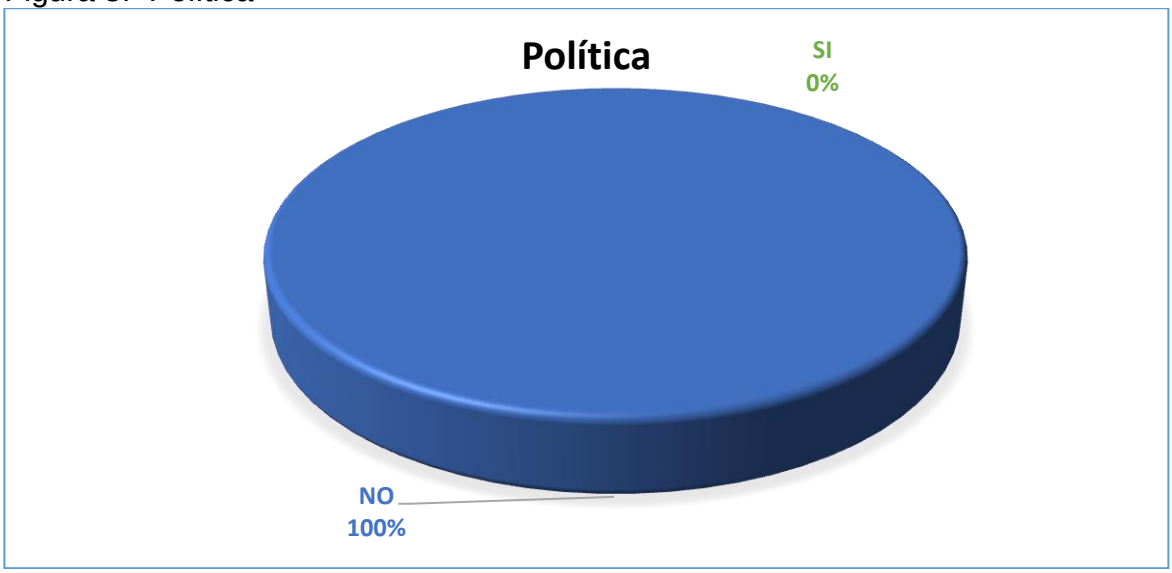
- Un SGSI sin recursos en el momento adecuado no podrá cumplir sus objetivos, la parte gerencial debe garantizar que los recursos estén disponibles cuando sea necesario.

- La alta dirección debe definir la política de seguridad de la información dentro del alcance del SGSI. La política necesita ser apropiada a sus actividades, incluir un compromiso de mejora continua y proporcionar objetivos o un marco para su establecimiento.

- Sin embargo, la responsabilidad y autoridad debe ser asignada por la alta dirección para organizar las actividades de seguridad de la información.

4.5.3 Política

Figura 8. Política



Fuente: Los Autores

Según resultados de la encuesta en la figura 8, política, se concluye que no existe una política de seguridad de la información definida, por lo tanto, se requiere que:

- La alta dirección debe definir la política de seguridad de la información dentro del alcance del SGSI. La política necesita ser apropiada a sus actividades, incluir un compromiso de mejora continua y proporcionar objetivos o un marco para su establecimiento.

- La política debe ser documentada, comunicada a los empleados y estar a disposición de otras partes interesadas.

2.5.4 Planificación

Figura 9. Planificación

Fuente: Los Autores

En la figura 9, planificación, se tiene un 100 % de no cumplimiento para planificar los riesgos de seguridad. Debe existir un proceso que establezca y mantenga los criterios de riesgo, así como identifica, analiza y evalúa los riesgos de seguridad de la información, además, se debe tener claro los actores más importantes que están involucrados en la protección de la información y cómo será evaluado.

2.5.5 Soporte

Figura 10. Soporte

Fuente: Los Autores

En la figura 10, soporte, se denota que para el proceso de soporte, existe un cumplimiento positivo a la fecha del 60 % y el restante, corresponde a un 40 % de no cumplimiento de estos procesos. Se encuentra que:

- Los recursos (Por ejemplo, equipos, instalaciones, dinero, etc.) deben estar disponibles para el establecimiento, implementación, operación y mejora continua del SGSI.

- La competencia es evaluada, y la capacitación, para el personal que realiza tareas que puedan afectar a la seguridad de la información.

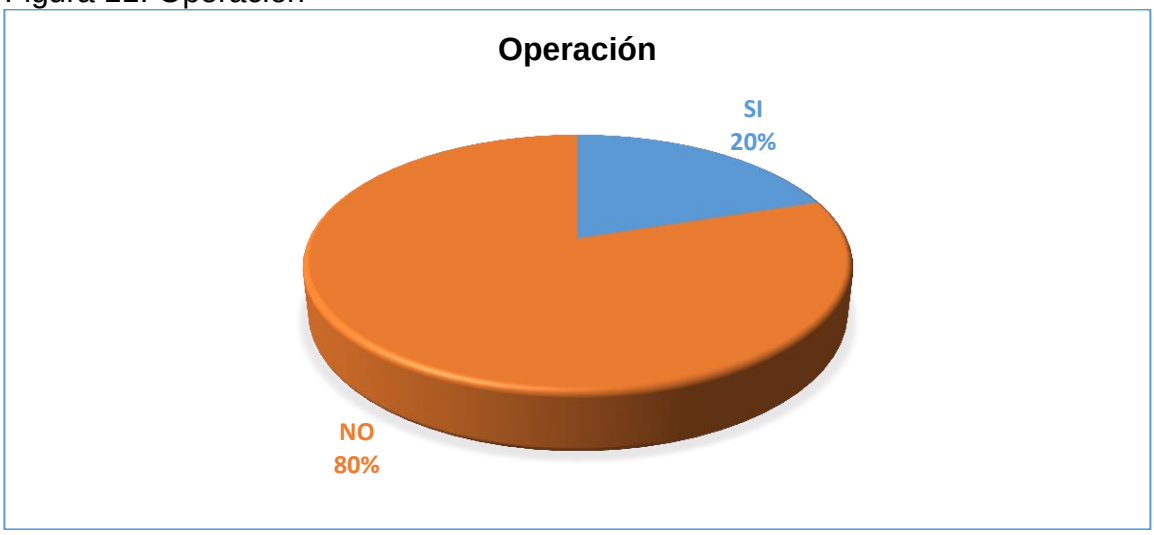
- Existe un proceso de comunicación interno y externo en la empresa.

- Existe un procedimiento para el control de los documentos que especifique la aprobación, revisión, actualización, identificación, la disponibilidad de la versión correspondiente, legibilidad del documento, control de documentos externos y la prevención de uso de documentos obsoletos.

- La información documentada externa manejada por la organización, debe ser controlada y protegida de la misma manera que la interna.

2.5.6 Operación

Figura 11. Operación



Fuente: Los Autores

La figura 11, operación, muestra un 20 % de cumplimiento en contra de un 80% que no corresponde a seguimientos positivos, para esto se concluye lo siguiente:

- La información documentada debe mantenerse para tener constancia de que los procesos se han llevado a cabo como estaba previsto (por ejemplo, procedimientos de control operacional, criterios de funcionamiento, etc.).

- Para minimizar los riesgos de seguridad de la información, los cambios deben ser controlados.

- Se debe realizar una evaluación de la seguridad y las evidencias deben ser registradas.

- Tienen que existir planes para lograr los objetivos y metas, éstos deben incluir responsabilidades, método de evaluación, los medios y plazos para el plan.

- Es necesario establecer acciones para tratar los riesgos considerados como no aceptables. Estas acciones necesitan ser implementadas, revisadas y controladas periódicamente siempre que sea posible.

2.5.7 Evaluación del desempeño

Figura 12. Evaluación del desempeño

Fuente: Los Autores

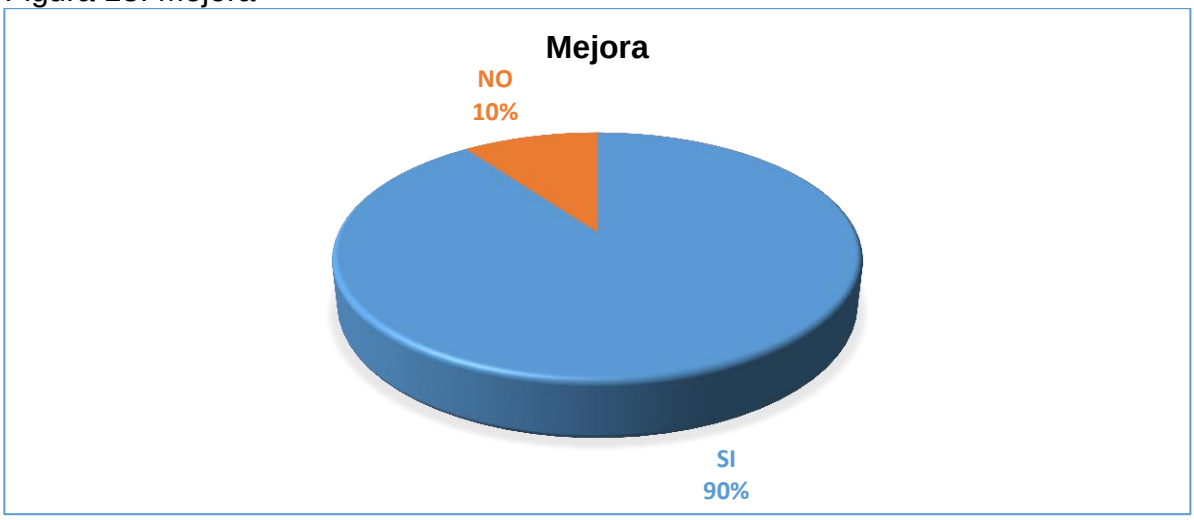
En la figura 12, evaluación del desempeño, los resultados no son favorables, generando solo un 10% de cumplimiento y un 90 % de saldo negativo, lo que conlleva a:

- Los resultados de medición deben ser documentados, analizados y evaluados por personas responsables.

- Los procedimientos de auditoría deben abordar las responsabilidades de auditoría, informes, criterios, frecuencia, alcance y los métodos. Los procedimientos deben incluir criterios para la selección de auditores y así mantener la imparcialidad y la objetividad.

2.5.8 Mejora

Figura 13. Mejora



Fuente: Los Autores

En la figura 13, en los procesos de mejora se tienen una visión positiva de un 90 %, lo que da como resultado que en la actualidad se dispone de buenas prácticas de mejora y se deja constancia de lo siguiente:

- Existe un procedimiento para tratar las no conformidades, incluyendo la adopción de medidas correctivas.

- El procedimiento debe incluir la identificación, investigación, determinación de causas y acciones, para prevenir la recurrencia. Estas acciones deben ser adecuadas a la magnitud de la no conformidad.

- Los registros deben mantenerse y la evaluación de la efectividad de las acciones correctivas. Deben hacerse los cambios necesarios en la documentación del SGSI.

3. DISEÑO METODOLÓGICO

3.1 SELECCIÓN METODOLOGÍA

Se selecciona Magerit al ser una metodología práctica y sistemática para gestionar riesgos derivados del uso de tecnologías de la información y la comunicación, con el fin de implementar medidas de control adecuadas que permitan mitigar los riesgos a los que están expuestos los activos de información. Esta metodología presenta una guía paso a paso de cómo llevar a cabo el análisis de riesgos.

3.2 ANÁLISIS DE RIESGOS

Toda organización se encuentra expuesta a riesgos; ya que en su entorno y en ella misma hay vulnerabilidades que pueden ser explotadas de no ser tratadas de manera adecuada, de ahí la importancia que la organización esta alerta ante cualquier cambio que pueda afectar algún activo de información.

Mediante el análisis de riesgos se pretenden alcanzarlos siguientes objetivos:

- Determinar los activos más significativos que posee la empresa.
- Establecer las amenazas a las que están expuestos cada activo.
- Escoger los controles de la norma NTC-ISO-IEC 27001:2013 apropiadas para los activos.
- Estimar el impacto si se materializara alguna amenaza.

3.3 CARACTERIZACIÓN DE LOS ACTIVOS DEL SISTEMA DE COPIAS DE RESPALDO

3.3.1 Identificación de activos. En esta actividad se identificaron los activos de información del servidor de copias de respaldo de la entidad, Estos son los bienes tangibles e intangibles que tiene la empresa para que el desempeño sea óptimo. Como se presenta en el cuadro 2, inventario de activos de información.

Los activos de Magerit se clasifican en:

- Software
- Hardware
- Personal
- Redes/Comunicaciones
- Infraestructura

Cuadro 2. Inventario de activos de información

Activos	Descripción
Aplicaciones	
Heon	Sistema de información para los procesos médicos
Sistema operativo	Windows 7 ultimate - Windows server 2000 - Windows Xp – Linux
Ofimática	Microsoft Office 2010 Standard
Antivirus	Antivirus gratuito - 360 Security
Servidor de Correo	Cpayweb - dominio: corvesalud.com.co
Navegador web	Página empresarial - Dominio corvesalud.com.co
Equipos	
Equipos de computo	Equipos medianos
Servidor Windows	Servidor del control de entrada y cuentas medicas - sistema de backups
Servidor Linux	Servidor para el cargue de Nomina
Impresoras	Equipos medianos
Routers	Equipos para conexión de red
Switches	Equipos para conexión de red
Equipos biomédicos	Equipos de uso médico
Escáneres	Equipos pequeños
Módems	Equipos para conexión de red
Discos duros	Dispositivos de almacenamiento
Memorias USB	Dispositivos USB
Redes/ Comunicaciones	
Red LAN	Red cableada
Red WIFI	Red inalámbrica
Internet	Red para conexión
Red Telefónica	Plantas telefónicas
Infraestructura	
Edificio Administrativo	Edificaciones
Edificios asistenciales	Edificaciones
Plataformas móviles	Plataformas móviles
Vehículo terrestre	Vehículo terrestre (Carro - Moto)
Cableado	Cableado estructurado - eléctrico

Cuadro 2. (Continuación)

Activos	Descripción
Infraestructura	
Camillas	Equipos mobiliarios
Escritorios	Equipos mobiliarios
Sillas	Equipos mobiliarios
Personal	
Administrativos	Usuarios Internos
Médicos generales	Usuarios Internos
Odontólogos	Usuarios Internos
Usuarios	Usuarios Externos
Proveedores	Proveedores

Fuente: Los Autores

- **Software.** Hace referencia a los programas, aplicaciones y desarrollos recopilados en la empresa para la automatización de la misma.

- **Hardware**. Se refiere a los bienes físicos que se usan en la empresa y son reemplazados si se presenta alguna incidencia.

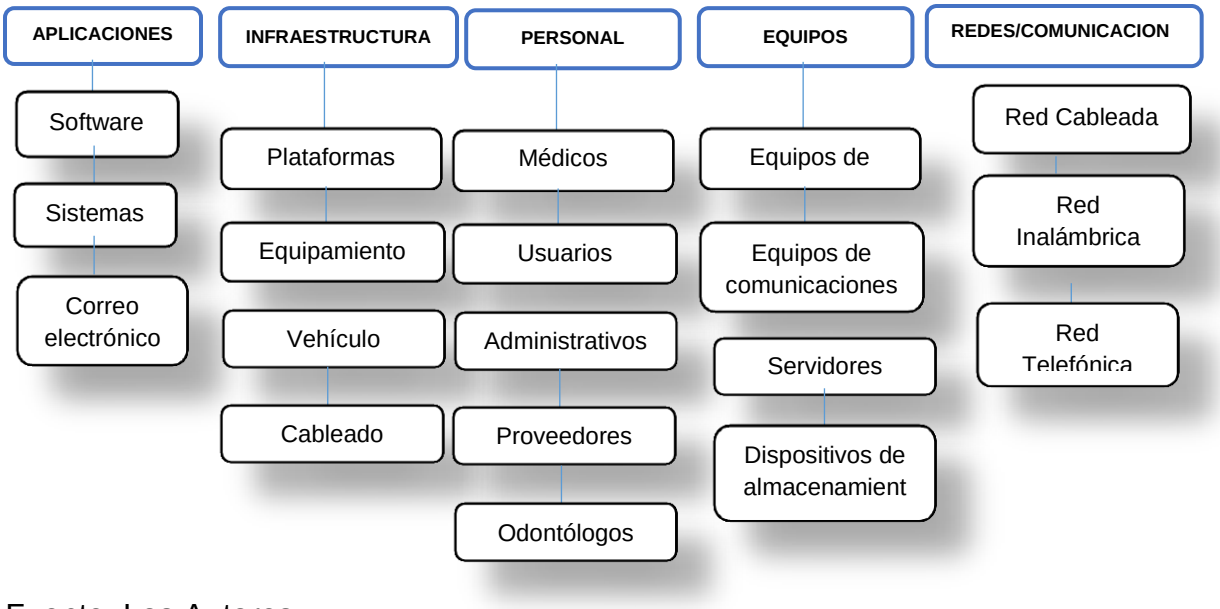
- **Personal.** Se refiere a las personas involucradas en los procesos y sistemas de información de la empresa.

- **Redes/Comunicaciones.** Hacen referencia a los servicios contratados a terceros.

- **Infraestructura.** La infraestructura se refiere a los lugares o instalaciones donde está alojado todo lo relacionado con los equipos tecnológicos, de oficina y médicos.

3.3.2 Dependencias entre activos. Estas relacionan los activos de manera jerarquizada evaluando el grado en que están vinculados entre sí, y en función de los parámetros disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. En la figura 14, mapa de dependencias entre activos se relacionan los activos correspondientes al proceso del servidor de copias de respaldo.

Figura 14 . Mapa de dependencias entre activos



Fuente: Los Autores

3.3.3 Valoración de los activos. Una vez identificados los activos se valoró su grado de importancia y criticidad para la entidad, teniendo en cuenta la afectación y pérdida que le puede generar a la organización desde el punto de vista económico, legal y de imagen, en caso tal que se materialice alguna amenaza y esta afecte su disponibilidad, integridad o confidencialidad. Para tal efecto, se utilizaron los siguientes criterios para realizar la respectiva valoración. En el cuadro 3, criterios de valoración se definen los criterios y su respectiva valoración.

Cuadro 3. Criterios de valoración

Valor		Criterio
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	Alto	daño grave
3-5	Medio	daño importante
1-2	Bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, Proyectos de análisis de riegos. Magerit – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro II – Catálogo de elementos, 20112 p. 19.

Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

En el cuadro 4, valoración de activos se enumeran los activos que pertenecen al proceso del servidor de copias de respaldo, evaluando la criticidad en cada dimensión.

Cuadro 4. Valoración de activos

	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Aplicaciones					
Heon	10	10	10	10	10
Sistema operativo	3	4	4	4	5
Ofimática	0	1	0	0	1
Antivirus	5	6	5	4	5
Servidor de Correo	7	8	8	7	6
Navegador web	5	5	4	4	6

Cuadro 4. (Continuación)

	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Equipos					
Equipos de computo	4	3	4	2	3
Servidor Windows	9	9	9	9	9
Servidor Linux	9	9	9	9	9
Impresoras	1	0	0	0	1
Routers	8	7	7	6	8
Switches	8	7	7	6	8
Equipos biomédicos	7	4	4	2	2
Escáneres	1	0	0	0	1
Módems	5	4	4	3	4
Discos duros	9	9	9	9	9
Memorias USB	9	9	9	9	9
Redes/ Comunicaciones					
Red LAN	8	8	8	7	8
Red WIFI	8	8	8	7	8
Internet	8	8	8	7	8
Red Telefónica	5	5	5	4	4
Infraestructura					
Edificio Administrativo	8	8	6	6	8
Edificios asistenciales	8	8	6	6	8
Plataformas móviles	6	4	3	3	3
Vehículo terrestre	2	2	1	1	2
Cableado	4	4	3	3	5
Camillas	2	1	1	1	2
Escritorios	0	0	0	0	1
Sillas	0	0	0	0	1
Personal					
Administrativos	9	9	9	9	9
Médicos generales	9	9	9	9	9
Odontólogos	9	9	9	9	9
Usuarios	9	9	9	9	9
Proveedores	8	7	7	8	8

Fuente: Los Autores

3.4 CARACTERIZACIÓN DE LAS AMENAZAS

Para facilitar la identificación de estas amenazas, en el Cuadro 5. Inventario de amenazas se lista una serie de amenazas de seguridad que en términos generales pueden afectar la organización y su sistema de gestión de la seguridad de la información, evaluando lo que pueda pasar, que consecuencias se derivan y que tan probable es que pase. El catálogo de elementos clasifica las amenazas en cuatro grupos.

- [N] Desastres Naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataque intencionados

En el cuadro 5, catálogo de amenazas se listan cada una de las amenazas con su respectiva descripción.

Cuadro 5. Catálogo de Amenazas

Catálogo de amenazas	
[N] Desastres naturales	
Identificador	**Descripción**
[N.1] Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[N.2] Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema.
[N.*] Desastres naturales	Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras,…

Cuadro 5. (Continuación)

Catálogo de amenazas	
[I] De origen industrial	
Identificador	**Descripción**
[I.1] Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
[I.2] Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
[I.*] Desastres industriales	otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico,
[I.3] Contaminación mecánica	vibraciones, polvo, suciedad, ...
[I.4] Contaminación electromagnética	interferencias de radio, campos magnéticos, luz ultravioleta, ...
[I.5] Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I] De origen industrial	
Identificador	**Descripción**
[I.6] Corte del suministro eléctrico	Cese de la alimentación de potencia
[I.7] Condiciones inadecuadas de temperatura o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad,...
[I.8] Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
[I.9] Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ...

Cuadro 5. (Continuación)

Catálogo de amenazas	
[I] De origen industrial	
Identificador	**Descripción**
[I.10] Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo
[I.11] Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.
[E] Errores y fallos no intencionados	
Identificador	**Descripción**
[E.1] Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación
[E] Errores y fallos no intencionados	
Identificador	**Descripción**
[E.3] Errores de monitorización (log)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos,...
[E.4] Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
[E.7] Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
[E.8] Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

Cuadro 5. (Continuación)

Catálogo de amenazas	
[E] Errores y fallos no intencionados	
Identificador	**Descripción**
[E.9] Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
[E.10] Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.
[E.14] Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
[E.15] Alteración accidental de la información	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[E.18] Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[E.19] Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.
[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
[E] Errores y fallos no intencionados	
Identificador	**Descripción**
[E.21] Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

Cuadro 5. (Continuación)

Catálogo de amenazas	
[E] Errores y fallos no intencionados	
Identificador	**Descripción**
[E.24] Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[E.25] Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
[E.28] Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica,...
[A] Ataques intencionados	
Identificador	**Descripción**
[A.3] Manipulación de los registros de actividad (log)	No tiene
[A.4] Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
[A.5] Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.
[A.6] Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[A] Ataques intencionados	
Identificador	**Descripción**
[A.7] Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

Cuadro 5. (Continuación)

Catálogo de amenazas	
[A] Ataques intencionados	
Identificador	**Descripción**
[A.8] Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
[A.9] [Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
[A.10] Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.
[A.11] Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
[A.12] Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.
[A.13] Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.
[A.14] Interceptación de información (escucha)	Atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
[A.15] Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
[A.18] Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
[A] Ataques intencionados	
Identificador	**Descripción**
[A.19] Divulgación de información	Revelación de información.
[A.22] Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

Cuadro 5. (Continuación)

Catálogo de amenazas	
[A] Ataques intencionados	
Identificador	**Descripción**
[A.23] Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[A.24] Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.25] Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
[A.26] Ataque destructivo	Vandalismo, terrorismo, acción militar, ...
[A.27] Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.
[A.28] Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos,...
[A.29] Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
[A.30] Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Fuente: MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, Proyectos de análisis de riegos, Magerit – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro II – Catálogo de elementos, 2012, p. 25 - 47.

Esta actividad consta de 2 sub-tareas:

- Identificación de las amenazas
- Valoración de las amenazas

3.4.1 Identificación de las amenazas. En el cuadro 6, identificación de amenazas, se identifican las amenazas relevantes sobre cada activo de la entidad.

Cuadro 6. Identificación de amenazas

Activos	Amenaza
Heon	[I.5] Avería de origen físico o lógico
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.5] Suplantación de la identidad del usuario
Sistema operativo	[I.5] Avería de origen físico o lógico
	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.7] Uso no previsto
Ofimática	[E.1] Errores de los usuarios
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.8] Difusión de software dañino
Antivirus	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[I.5] Avería de origen físico o lógico
	[I.8] Fallo de servicios de comunicaciones
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto

Cuadro 6. (Continuación)

Activos	Amenaza
Navegador web	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[I.5] Avería de origen físico o lógico
	[I.8] Fallo de servicios de comunicaciones
	[I.6] Corte de suministro eléctrico
Equipos de computo	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
Servidor Windows	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware

Cuadro 6. (Continuación)

Activos	Amenaza
Servidor Linux	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
Impresoras	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.11] Acceso no autorizado
Routers	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[A.11] Acceso no autorizado
Switches	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[A.11] Acceso no autorizado

Cuadro 6. (Continuación)

Activos	Amenaza
Equipos biomédicos	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
Escáneres	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
Módems	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
Discos duros	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[A.*] Ataques intencionados
	[E.*] errores y fallos no intencionados
	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.*] errores y fallos no intencionados

Cuadro 6. (Continuación)

Activos	Amenaza
Red LAN	[I.8] Fallo de servicios de comunicaciones
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de secuencia
	[A.5] Suplantación de la identidad del usuario
	[A.9] [Re-]encaminamiento de mensajes
	[A.10] Alteración de secuencia
	[A.11] Acceso no autorizado
Red WIFI	[I.8] Fallo de servicios de comunicaciones
	[E.9] Errores de [re-]encaminamiento
Internet	[I.8] Fallo de servicios de comunicaciones
	[A.7] Uso no previsto
Red Telefónica	[I.8] Fallo de servicios de comunicaciones
	[A.5] Suplantación de la identidad del usuario
	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[N.1] Fuego
	[N.2] Daños por agua
	[N.*.1] Tormentas
	[N.*.4] Terremotos
	[N.*.9] Tsunamis
	[N.*.11] Calor extremo
	[I.*] Desastres industriales
	[A.27] Ocupación enemiga

Cuadro 6. (Continuación)

Activos	Amenaza
Edificios asistenciales	[N.1] Fuego
	[N.2] Daños por agua
	[N.*.1] Tormentas
	[N.*.4] Terremotos
	[N.*.9] Tsunamis
	[N.*.11] Calor extremo
	[I.*] Desastres industriales
	[A.27] Ocupación enemiga
Plataformas móviles	[I.8] Fallo de servicios de comunicaciones
	[A.5] Suplantación de la identidad del usuario
	[N.2] Daños por agua
	[I.5] Avería de origen físico o lógico
Vehículo terrestre	[N.1] Fuego
	[N.2] Daños por agua
	[N.*.11] Calor extremo
	[I.*] Desastres industriales
Cableado	[I.3] Contaminación medioambiental
	[I.7] Condiciones inadecuadas de temperatura o humedad
Camillas	[I.3] Contaminación medioambiental
	[N.1] Fuego
	[N.2] Daños por agua
Escritorios	[I.3] Contaminación medioambiental
	[N.1] Fuego
	[N.2] Daños por agua
	[I.3] Contaminación medioambiental
	[N.1] Fuego
	[N.2] Daños por agua
	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)
	[E.28.1] Enfermedad

Cuadro 6. (Continuación)

Activos	Amenaza
Médicos generales	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)
	[E.28.1] Enfermedad
Odontólogos	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)
	[E.28.1] Enfermedad
Usuarios	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)
	[E.28.1] Enfermedad
Proveedores	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)
	[E.28.1] Enfermedad

Fuente: Los Autores

3.4.2 Valoración de las amenazas. La valoración de amenazas tiene como objetivos:

- Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo.

- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Para realizar la tarea de valoración de las amenazas de cada activo se ha tomado en cuenta la degradación de valor y la probabilidad de ocurrencia. En el cuadro 7, degradación de valor y la probabilidad de ocurrencia, teniendo en cuenta los parámetros de *muy raro* cuando la probabilidad de ocurrencia es casi nula, *poco probable* en caso de que el resultado tenga muy pocas probabilidades de ocurrir, *posible* en el momento en que la probabilidad existe o que pueda suceder, *probable* en el tiempo en que es seguro que pueda suceder y prácticamente seguro en el punto en que es un hecho que ocurrió la probabilidad del evento; se observa la escala de valores que se van a tener en cuenta durante la valoración de las amenazas.

Cuadro 7. Degradación de valor y la probabilidad de ocurrencia

Degradación de valor		Probabilidad de ocurrencia	
MB	Muy Bajo	**MB**	Muy Raro
B	Bajo	**B**	Poco probable
M	Medio	**M**	Posible
A	Alto	**A**	Probable
MA	Muy Alto	**MA**	prácticamente seguro

Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro III – Guía de técnicas, 2012. p. 6.

En el cuadro 8, valoración de amenazas por activo, muestra el listado de activos y amenazas y su respectiva valoración.

Cuadro 8. Valoración de amenazas por activo

Activos	Amenaza	P	[D]	[I]	[C]	[A]	[T]
Heon	[I.5] Avería de origen físico o lógico	M	A	A	A	A	A
	[E.20] Vulnerabilidades de los programas (software)	MB	MA	MA	MA	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	MA	A	A	MA	M
	[A.5] Suplantación de la identidad del usuario	A	A	MA	A	MA	B
Sistema operativo	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[E.1] Errores de los usuarios	MA	A	A	A	MA	A
	[E.8] Difusión de software dañino	M	MA	MA	MA	A	A
	[E.20] Vulnerabilidades de los programas (software)	MB	MA	MA	MA	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	MA	A	A	MA	M
	[A.7] Uso no previsto	M	A	A	A	A	M
Ofimática	[E.1] Errores de los usuarios	A	MA	A	A	MA	M
	[E.20] Vulnerabilidades de los programas (software)	MB	MA	MA	MA	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	MA	MA	A	A	MA	M
	[A.8] Difusión de software dañino	M	M	M	M	M	B
Antivirus	[E.8] Difusión de software dañino	M	MA	MA	MA	A	A
	[E.20] Vulnerabilidades de los programas (software)	MB	MA	MA	MA	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	MA	A	A	MA	M

Cuadro 8. (Continuación)

Activos	Amenaza	P	[D]	[I]	[C]	[A]	[T]
Navegador web	[E.1] Errores de los usuarios	A	A	A	A	MA	A
	[E.8] Difusión de software dañino	M	MA	MA	MA	A	A
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.8] Fallo de servicios de comunicaciones	MA	A	M	B	M	A
	[I.6] Corte de suministro eléctrico	M	A	B	B	B	M
Servidor de Correo	[E.1] Errores de los usuarios	A	A	A	A	MA	A
	[E.8] Difusión de software dañino	M	MA	MA	MA	A	A
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.8] Fallo de servicios de comunicaciones	MA	A	M	B	M	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	MA	A	A	MA	M
	[A.6] Abuso de privilegios de acceso	A	M	A	MA	A	M
	[A.7] Uso no previsto	A	A	A	A	A	M
Equipos de computo	[N.2] Daños por agua	M	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.*] Desastres industriales	B	MA	B	B	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A	M	B	MB	B
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	MA	A	A	MA	M
	[E.24] Caída del sistema por agotamiento de recursos	A	A	M	M	A	M
	[A.6] Abuso de privilegios de acceso	MA	A	A	MA	MA	M
	[A.7] Uso no previsto	MA	A	A	A	A	M
Servidor Windows	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A	M	B	MB	B
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	MA	MA	MA	M
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	MA	A	A	MA	M
	[A.11] Acceso no autorizado	A	MA	MA	MA	A	M
	[A.23] Manipulación del hardware	M	A	MA	A	A	M

Cuadro 8. (Continuación)

Activos	Amenaza	P	[D]	[I]	[C]	[A]	[T]
Servidor Linux	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A	M	B	MB	B
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	MA	MA	MA	M
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	MA	A	A	MA	M
	[A.11] Acceso no autorizado	A	MA	MA	MA	A	M
	[A.23] Manipulación del hardware	M	A	MA	A	A	M
Impresoras	[I.5] Avería de origen físico o lógico	MA	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A	M	B	MB	B
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	MA	A	A	MA	M
	[A.11] Acceso no autorizado	B	MA	MA	MA	A	M
Routers	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A	M	B	MB	B
	[A.11] Acceso no autorizado	A	MA	MA	MA	A	M
Switches	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	M	B	MB	B
	[A.11] Acceso no autorizado	A	MA	MA	MA	A	M
Equipos biomédicos	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	M	B	MB	B

Cuadro 8. (Continuación)

Activos	Amenaza	P	[D]	[I]	[C]	[A]	[T]
Escáneres	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	M	B	MB	B
Módems	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	M	B	MB	B
Discos duros	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	M	B	MB	B
	[A.*] Ataques intencionados	M	A	A	A	A	M
	[E.*] Errores y fallos no intencionados	A	A	A	A	M	B
Memorias USB	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	M	B	MB	B
	[E.*] Errores y fallos no intencionados	M	A	A	A	M	B
Red LAN	[I.8] Fallo de servicios de comunicaciones	A	A	M	B	M	A
	[E.9] Errores de [re-]encaminamiento	M	A	A	A	M	B
	[E.10] Errores de secuencia	M	A	A	A	M	B
	[A.5] Suplantación de la identidad del usuario	B	A	MA	MA	A	MB
	[A.9] [Re-]encaminamiento de mensajes	M	A	A	A	M	B
	[A.10] Alteración de secuencia	B	A	A	A	M	B
	[A.11] Acceso no autorizado	A	MA	MA	MA	A	M
Red WIFI	[I.8] Fallo de servicios de comunicaciones	A	A	M	B	M	A
	[E.9] Errores de [re-]encaminamiento	B	A	A	A	M	B

Cuadro 8. (Continuación)

Activos	Amenaza	P	[D]	[I]	[C]	[A]	[T]
Internet	[I.8] Fallo de servicios de comunicaciones	A	A	M	B	M	A
	[A.7] Uso no previsto	B	A	A	A	A	M
Red Telefónica	[I.8] Fallo de servicios de comunicaciones	A	A	M	B	M	A
	[A.5] Suplantación de la identidad del usuario	B	A	MA	MA	A	MB
	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*] Desastres naturales	MB	MA	B	B	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
Edificio Administrativo	[N.1] Fuego	A	MA	B	B	B	B
	[N.2] Daños por agua	A	MA	B	B	B	B
	[N.*.1] Tormentas	A	MA	B	B	B	B
	[N.*.4] Terremotos	B	MA	B	B	B	B
	[N.*.9] Tsunamis	MB	MA	B	B	B	B
	[N.*.11] Calor extremo	M	B	B	B	MB	B
	[I.*] Desastres industriales	B	A	B	B	B	B
	[A.27] Ocupación enemiga	B	M	M	M	B	B
Edificios asistenciales	[N.1] Fuego	A	MA	B	B	B	B
	[N.2] Daños por agua	A	MA	B	B	B	B
	[N.*.1] Tormentas	A	MA	B	B	B	B
	[N.*.4] Terremotos	B	MA	B	B	B	B
	[N.*.9] Tsunamis	MB	MA	B	B	B	B
	[N.*.11] Calor extremo	M	B	B	B	MB	B
	[I.*] Desastres industriales	B	A	B	B	B	B
	[A.27] Ocupación enemiga	B	M	M	M	B	B
Plataformas móviles	[I.8] Fallo de servicios de comunicaciones	A	A	M	B	M	A
	[A.5] Suplantación de la identidad del usuario	B	A	MA	MA	A	MB
	[N.2] Daños por agua	B	MA	B	B	B	B
	[I.5] Avería de origen físico o lógico	A	MA	A	A	A	MB
Vehículo terrestre	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
	[N.*.11] Calor extremo	B	B	B	B	MB	B
	[I.*] Desastres industriales	MB	A	B	B	B	B
Cableado	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A	M	B	MB	B

Cuadro 8. (Continuación)

Activos	Amenaza	P	[D]	[I]	[C]	[A]	[T]
Camillas	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
Escritorios	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
Sillas	[I.3] Contaminación medioambiental	B	A	A	M	B	B
	[N.1] Fuego	B	MA	B	B	B	B
	[N.2] Daños por agua	B	MA	B	B	B	B
Administrativos	[A.29] Extorsión	MB	M	A	A	A	B
	[A.30] Ingeniería social (picaresca)	A	B	A	MA	MA	M
	[E.28.1] Enfermedad	A	A	A	MB	MB	MB
Médicos generales	[A.29] Extorsión	MB	M	A	A	A	B
	[A.30] Ingeniería social (picaresca)	A	B	A	MA	MA	M
	[E.28.1] Enfermedad	A	A	A	MB	MB	MB
Odontólogos	[A.29] Extorsión	MB	M	A	A	A	B
	[A.30] Ingeniería social (picaresca)	A	B	A	MA	MA	M
	[E.28.1] Enfermedad	A	A	A	MB	MB	MB
Usuarios	[A.29] Extorsión	MB	M	A	A	A	B
	[A.30] Ingeniería social (picaresca)	A	B	A	MA	MA	M
	[E.28.1] Enfermedad	A	A	A	MB	MB	MB
Proveedores	[A.29] Extorsión	MB	M	A	A	A	B
	[A.30] Ingeniería social (picaresca)	A	B	A	MA	MA	M
	[E.28.1] Enfermedad	A	A	A	MB	MB	MB

***P**: Probabilidad, **D**: Disponibilidad, **I:**Integridad; **C**:Confidencialidad; **A:** Autenticidad, **T**:Trazabilidad*

Fuente: Los Autores

En el anterior cuadro, se calcula la estimación del impacto en donde los activos que obtienen una calificación de **MA** son los que requieren atención inmediata. Por otra parte, se calcula el riesgo, para esto se modela el impacto y la probabilidad, por medio de los valores del cuadro 9, cálculo del riesgo.

Cuadro 9. Calculo del riesgo

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto [5]	**MA:** prácticamente seguro [5]	**MA:** crítico [5]
A: alto [4]	**A:** probable [4]	**A:** importante [4]
M: medio [3]	**M:** posible [3]	**M:** apreciable [3]
B: bajo [2]	**B:** poco probable [2]	**B:** bajo [2]
MB: muy bajo [1]	**MB:** muy raro [1]	**MB:** despreciable [1]

Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, Magerit – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro III – Guía de técnicas, 2012. p. 6.

Se combina el impacto y la frecuencia o probabilidad para calcular el riesgo, En el cuadro 10, mapa de calor de riesgo se observa esta combinación.

Cuadro 10. Mapa de calor de riesgo = Impacto * Probabilidad

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, Magerit – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro III – Guía de técnicas, 2012. p. 6.

En el cuadro 11, evaluación de riesgos, se muestran los resultados obtenidos en la valoración del riesgo de cada amenaza.

Cuadro 11. Evaluación de riesgos

Activos	**Amenaza**	**P**	**Valoración Impacto**						**R**
			[D]	**[I]**	**[C]**	**[A]**	**[T]**	**prom**	
Heon	[I.5] Avería de origen físico o lógico	**3**	4	4	4	4	4	**4**	**12**
	[E.20] Vulnerabilidades de los programas (software)	**1**	5	5	5	4	4	**5**	**5**
	[E.21] Errores de mantenimiento / actualización de programas (software)	**3**	5	4	4	5	3	**4**	**13**
	[A.5] Suplantación de la identidad del usuario	**4**	4	5	4	5	2	**4**	**16**

Cuadro 11. (Continuación)

Activos	Amenaza	P	Valoración Impacto						R
			[D]	[I]	[C]	[A]	[T]	prom	
Sistema operativo	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[E.1] Errores de los usuarios	5	4	4	4	5	4	4	21
	[E.8] Difusión de software dañino	3	5	5	5	4	4	5	14
	[E.20] Vulnerabilidades de los programas (software)	1	5	5	5	4	4	5	5
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	5	4	4	5	3	4	17
	[A.7] Uso no previsto	3	4	4	4	4	3	4	11
Ofimática	[E.1] Errores de los usuarios	4	5	4	4	5	3	4	17
	[E.20] Vulnerabilidades de los programas (software)	1	5	5	5	4	4	5	5
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	5	4	4	5	3	4	21
	[A.8] Difusión de software dañino	3	3	3	3	3	2	3	8
Antivirus	[E.8] Difusión de software dañino	3	5	5	5	4	4	5	14
	[E.20] Vulnerabilidades de los programas (software)	1	5	5	5	4	4	5	5
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	5	4	4	5	3	4	17
Servidor de Correo	[E.1] Errores de los usuarios	4	4	4	4	5	4	4	17
	[E.8] Difusión de software dañino	3	5	5	5	4	4	5	14
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.8] Fallo de servicios de comunicaciones	5	4	3	2	3	4	3	16
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	5	4	4	5	3	4	17
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	4	3	2	1	2	2	2
	[A.6] Abuso de privilegios de acceso	4	3	4	5	4	3	4	15
	[A.7] Uso no previsto	4	4	4	4	4	3	4	15
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
Navegador web	[E.1] Errores de los usuarios	4	4	4	4	5	4	4	17
	[E.8] Difusión de software dañino	3	5	5	5	4	4	5	14
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.8] Fallo de servicios de comunicaciones	5	4	3	2	3	4	3	16
	[I.6] Corte de suministro eléctrico	3	4	2	2	2	3	3	8

Cuadro 11. (Continuación)

Activos	Amenaza	P	Valoración Impacto						R
			[D]	[I]	[C]	[A]	[T]	prom	
Equipos de computo	[N.2] Daños por agua	3	5	2	2	2	2	3	8
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.*] Desastres industriales	2	5	2	2	2	2	3	5
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	3	4	3	2	1	2	2	7
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	5	4	4	5	3	4	17
	[E.24] Caída del sistema por agotamiento de recursos	4	4	3	3	4	3	3	14
	[A.6] Abuso de privilegios de acceso	5	4	4	5	5	3	4	21
	[A.7] Uso no previsto	5	4	4	4	4	3	4	19
Servidor Windows	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	3	4	3	2	1	2	2	7
	[E.2] Errores del administrador del sistema / de la seguridad	4	4	5	5	5	3	4	18
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	5	4	4	5	3	4	17
	[A.11] Acceso no autorizado	4	5	5	5	4	3	4	18
	[A.23] Manipulación del hardware	3	4	5	4	4	3	4	12
Servidor Linux	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	3	4	3	2	1	2	2	7
	[E.2] Errores del administrador del sistema / de la seguridad	4	4	5	5	5	3	4	18
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	5	4	4	5	3	4	17
	[A.11] Acceso no autorizado	4	5	5	5	4	3	4	18
	[A.23] Manipulación del hardware	3	4	5	4	4	3	4	12

Cuadro 11. (Continuación)

Activos	Amenaza	P	Valoración Impacto						R
			[D]	[I]	[C]	[A]	[T]	prom	
Impresoras	[I.5] Avería de origen físico o lógico	5	5	4	4	4	1	4	18
	[I.7] Condiciones inadecuadas de temperatura o humedad	3	4	3	2	1	2	2	7
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	5	4	4	5	3	4	17
	[A.11] Acceso no autorizado	2	5	5	5	4	3	4	9
Routers	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	3	4	3	2	1	2	2	7
	[A.11] Acceso no autorizado	4	5	5	5	4	3	4	18
Switches	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	3	2	1	2	2	5
	[A.11] Acceso no autorizado	4	5	5	5	4	3	4	18
Equipos biomédicos	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	3	2	1	2	2	5
Escáneres	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	3	2	1	2	2	5

Cuadro 11. (Continuación)

Activos	Amenaza	P	Valoración Impacto						R
			[D]	[I]	[C]	[A]	[T]	prom	
Módems	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	3	2	1	2	2	5
Discos duros	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	3	2	1	2	2	5
	[A.*] Ataques intencionados	3	4	4	4	4	3	4	11
	[E.*] Errores y fallos no intencionados	4	4	4	4	3	2	3	14
Memorias USB	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	3	2	1	2	2	5
	[E.*] Errores y fallos no intencionados	3	4	4	4	3	2	3	10
Red LAN	[I.8] Fallo de servicios de comunicaciones	4	4	3	2	3	4	3	13
	[E.9] Errores de [re-]encaminamiento	3	4	4	4	3	2	3	10
	[E.10] Errores de secuencia	3	4	4	4	3	2	3	10
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	4	1	4	8
	[A.9] [Re-]encaminamiento de mensajes	3	4	4	4	3	2	3	10
	[A.10] Alteración de secuencia	2	4	4	4	3	2	3	7
	[A.11] Acceso no autorizado	4	5	5	5	4	3	4	18
Red WIFI	[I.8] Fallo de servicios de comunicaciones	4	4	3	2	3	4	3	13
	[E.9] Errores de [re-]encaminamiento	2	4	4	4	3	2	3	7

Cuadro 11. (Continuación)

Activos	Amenaza	P	Valoración Impacto						R
			[D]	[I]	[C]	[A]	[T]	prom	
Internet	[I.8] Fallo de servicios de comunicaciones	4	4	3	2	3	4	3	13
	[A.7] Uso no previsto	2	4	4	4	4	3	4	8
Red Telefónica	[I.8] Fallo de servicios de comunicaciones	4	4	3	2	3	4	3	13
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	4	1	4	8
	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*] Desastres naturales	1	5	2	2	2	2	3	3
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14
Edificio Administrativo	[N.1] Fuego	4	5	2	2	2	2	3	10
	[N.2] Daños por agua	4	5	2	2	2	2	3	10
	[N.*.1] Tormentas	4	5	2	2	2	2	3	10
	[N.*.4] Terremotos	2	5	2	2	2	2	3	5
	[N.*.9] Tsunamis	1	5	2	2	2	2	3	3
	[N.*.11] Calor extremo	3	2	2	2	1	2	2	5
	[I.*] Desastres industriales	2	4	2	2	2	2	2	5
	[A.27] Ocupación enemiga	2	3	3	3	2	2	3	5
Edificios asistenciales	[N.1] Fuego	4	5	2	2	2	2	3	10
	[N.2] Daños por agua	4	5	2	2	2	2	3	10
	[N.*.1] Tormentas	4	5	2	2	2	2	3	10
	[N.*.4] Terremotos	2	5	2	2	2	2	3	5
	[N.*.9] Tsunamis	1	5	2	2	2	2	3	3
	[N.*.11] Calor extremo	3	2	2	2	1	2	2	5
	[I.*] Desastres industriales	2	4	2	2	2	2	2	5
	[A.27] Ocupación enemiga	2	3	3	3	2	2	3	5
Plataformas móviles	[I.8] Fallo de servicios de comunicaciones	4	4	3	2	3	4	3	13
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	4	1	4	8
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[I.5] Avería de origen físico o lógico	4	5	4	4	4	1	4	14

Cuadro 11. (Continuación)

Activos	Amenaza	P	Valoración Impacto						R
			[D]	[I]	[C]	[A]	[T]	prom	
Vehículo terrestre	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
	[N.*.11] Calor extremo	2	2	2	2	1	2	2	4
	[I.*] Desastres industriales	1	4	2	2	2	2	2	2
Cableado	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[I.7] Condiciones inadecuadas de temperatura o humedad	3	4	3	2	1	2	2	7
Camillas	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
Escritorios	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	2	3	5
Sillas	[I.3] Contaminación medioambiental	2	4	4	3	2	2	3	6
	[N.1] Fuego	2	5	2	2	2	2	3	5
	[N.2] Daños por agua	2	5	2	2	2	B	3	6
Administrativos	[A.29] Extorsión	1	3	4	4	4	2	3	3
	[A.30] Ingeniería social (picaresca)	4	2	4	5	5	3	4	15
	[E.28.1] Enfermedad	4	4	4	1	1	1	2	9
Médicos generales	[A.29] Extorsión	1	3	4	4	4	2	3	3
	[A.30] Ingeniería social (picaresca)	4	2	4	5	5	3	4	15
	[E.28.1] Enfermedad	4	4	4	1	1	1	2	9
Odontólogos	[A.29] Extorsión	1	3	4	4	4	2	3	3
	[A.30] Ingeniería social (picaresca)	4	2	4	5	5	3	4	15
	[E.28.1] Enfermedad	4	4	4	1	1	1	2	9

Cuadro 11. (Continuación)

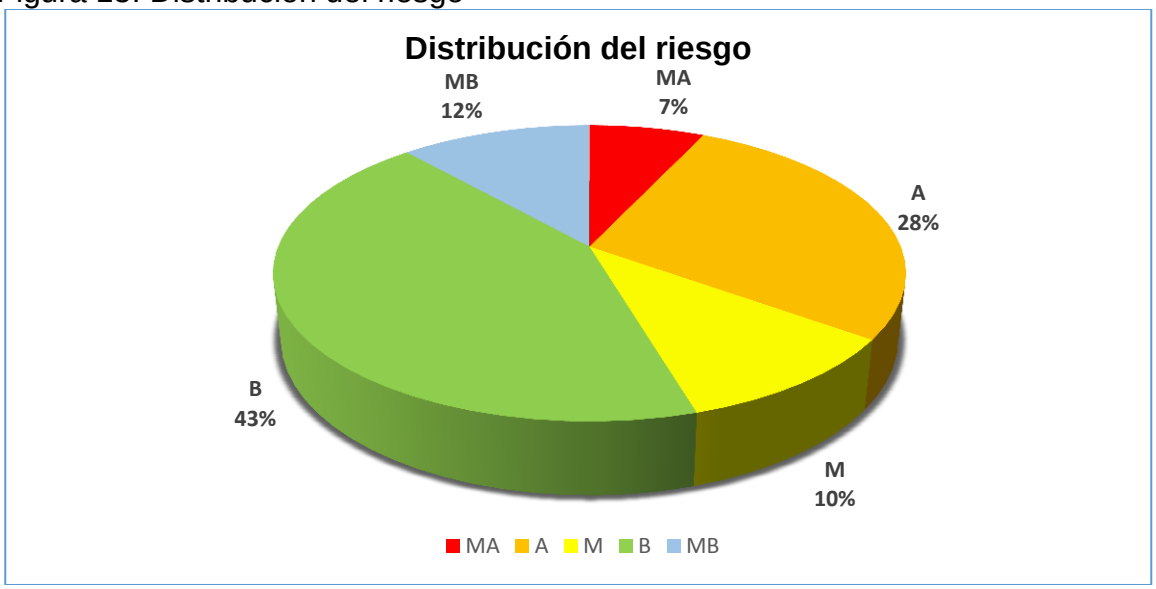
Activos	Amenaza	P	Valoración Impacto						R
			[D]	[I]	[C]	[A]	[T]	prom	
Usuarios	[A.29] Extorsión	1	3	4	4	4	2	3	3
	[A.30] Ingeniería social (picaresca)	4	2	4	5	5	3	4	15
	[E.28.1] Enfermedad	4	4	4	1	1	1	2	9
Proveedores	[A.29] Extorsión	1	3	4	4	4	2	3	3
	[A.30] Ingeniería social (picaresca)	4	2	4	5	5	3	4	15
	[E.28.1] Enfermedad	4	4	4	1	1	1	2	9

***R:** Riesgo, **P**: Probabilidad, **D**: Disponibilidad, **I:**Integridad; **C**:Confidencialidad; **A:** Autenticidad, **T**:Trazabilidad*

Fuente: Los Autores

Según la información recogida de los 34 activos evaluados con sus respectivas amenazas se obtiene la siguiente información, la cual es graficada en la figura 15, distribución del riesgo en el servidor de copias de respaldo. En la que se observa un 7% de riesgo muy alto y un 28% de riesgo alto en los activos de la entidad.

Figura 15. Distribución del riesgo



Fuente: Los Autores.

Los porcentajes correspondientes a *Nivel Alto* y *Medio Alto*, equivalen a un reflejo de la baja importancia que se les da a los activos que hacen referencia a la información, no existe conciencia enfatizada en la protección de la información de manera adecuada, además tampoco se destinan los recursos necesarios para el cuidado y protección de la misma. Se enfatizan estos valores ya que son los más sobresalientes y son los que requieren vigilancia continua que conlleven a un mejoramiento de los procesos para la protección y manejo de la información.

Para hallar un cálculo cuantitativo del riesgo total en los activos, tomamos como variables impacto por probabilidad y generando un rango de valores para establecerlos en que concesión está asignada. En el cuadro 12, rango de valores del riesgo se muestran las respectivas valoraciones.

Cuadro 12. Rango de valores del riesgo

Riesgo	Rango Min	Rango Max
MA	18	21
A	13	17
M	9	12
B	5	8
MB	1	4

Fuente: Los Autores

En el cuadro 13, criticidad de los activos se pueden verificar los activos que están siendo más afectados y a los cuales es importante aplicarles tratamientos de manera inmediata.

Cuadro 13. Criticidad de los activos.

	Aplicaciones	Equipos	Redes	Infraestructura	Personal
MA	***2***	***8***	***1***	0	0
A	***20***	***19***	***5***	2	5
M	2	4	3	6	5
B	6	40	7	23	0
MB	1	10	1	4	5
Total	**179**				

Fuente. Los Autores

Tomando como base el análisis de riesgo realizado, y según el cuadro de criticidad de los activos arroja los siguientes resultados diferenciados entre riesgos altos y muy altos. Corvesalud IPS dispone actualmente de 22 riesgos de amenazas a las aplicaciones que es un margen muy alto, lo que conlleva a que la seguridad y el manejo de las aplicaciones, no es óptimo. Por otra parte, se obtienen como resultado 27 amenazas dirigidas a los equipos de cómputo y servidores en los cuales se prioriza como alerta los accesos no autorizados y la manipulación de estos equipos de manera incorrecta. Se genera también un resultado no favorable hacia las redes y comunicaciones, tomando como información 6 tipos de amenazas que conllevan a fallos en servicios de red y que retrasan en ocasiones la operación de la empresa. Los datos generados también muestran un porcentaje significativo para cada uno de los tipos de activos valorados, distribuidos de la siguiente manera: Un valor del 71 % de las amenazas conceptualizadas para los activos de aplicaciones, un 33 % para los equipos y un

39 % de riesgos de amenazas que pueden afectar todo lo relacionado con las comunicaciones y redes. Todo lo anterior es causado por el uso intenso que se les da y que son canales directos para el acceso a la información de la empresa, generando un alto impacto de riesgo en el proceso de copias de respaldo. Por ende, son de vital importancia para el funcionamiento del servidor de copias de respaldo de la entidad.

Se encontraron 60 riesgos críticos que son afectados por las amenazas incluidas en el libro II- Catálogo de elementos de Magerit. En el cuadro 14, riesgos a trabajar se listan los riesgos encontrados mediante el análisis de riesgos.

Cuadro 14. Riesgos a trabajar

Activos	Amenaza	P	I	R
Heon	[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	13
	[A.5] Suplantación de la identidad del usuario	4	4	16
Sistema operativo	[I.5] Avería de origen físico o lógico	4	4	14
	[E.1] Errores de los usuarios	5	4	21
	[E.8] Difusión de software dañino	3	5	14
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	4	17
Ofimática	[E.1] Errores de los usuarios	4	4	17
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	4	21
Antivirus	[E.8] Difusión de software dañino	3	5	14
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	4	17
Navegador web	[E.1] Errores de los usuarios	4	4	17
	[E.8] Difusión de software dañino	3	5	14
	[I.5] Avería de origen físico o lógico	4	4	14
	[I.8] Fallo de servicios de comunicaciones	5	3	16
Servidor de Correo	[E.1] Errores de los usuarios	4	4	17
	[E.8] Difusión de software dañino	3	5	14
	[I.5] Avería de origen físico o lógico	4	4	14
	[I.8] Fallo de servicios de comunicaciones	5	3	16
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	4	17
	[A.6] Abuso de privilegios de acceso	4	4	15
	[A.7] Uso no previsto	4	4	15
	[I.5] Avería de origen físico o lógico	4	4	14
Equipos de computo	[I.5] Avería de origen físico o lógico	4	4	14
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	17
	[E.24] Caída del sistema por agotamiento de recursos	4	3	14
	[A.6] Abuso de privilegios de acceso	5	4	21
	[A.7] Uso no previsto	5	4	19

Cuadro 14. (Continuación)

Activos	Amenaza	P	I	R
Servidor Windows	[I.5] Avería de origen físico o lógico	4	4	14
	[E.2] Errores del administrador del sistema / de la seguridad	4	4	18
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	17
	[A.11] Acceso no autorizado	4	4	18
Servidor Linux	[I.5] Avería de origen físico o lógico	4	4	14
	[E.2] Errores del administrador del sistema / de la seguridad	4	4	18
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	17
	[A.11] Acceso no autorizado	4	4	18
Impresoras	[I.5] Avería de origen físico o lógico	5	4	18
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	17
Routers	[I.5] Avería de origen físico o lógico	4	4	14
	[A.11] Acceso no autorizado	4	4	18
Switches	[I.5] Avería de origen físico o lógico	4	4	14
	[A.11] Acceso no autorizado	4	4	18
Equipos Biomédicos	[I.5] Avería de origen físico o lógico	4	4	14
Escáneres	[I.5] Avería de origen físico o lógico	4	4	14
Módems	[I.5] Avería de origen físico o lógico	4	4	14
Datos disco duro	[I.5] Avería de origen físico o lógico	4	4	14
	[E.*] Errores y fallos no intencionados	4	3	14
Memorias USB	[I.5] Avería de origen físico o lógico	4	4	14
Red LAN	[I.8] Fallo de servicios de comunicaciones	4	3	13
	[A.11] Acceso no autorizado	4	4	18
Red WIFI	[I.8] Fallo de servicios de comunicaciones	4	3	13
Internet	[I.8] Fallo de servicios de comunicaciones	4	3	13
Red Telefónica	[I.8] Fallo de servicios de comunicaciones	4	3	13
	[I.5] Avería de origen físico o lógico	4	4	14
Plataformas móviles	[I.8] Fallo de servicios de comunicaciones	4	3	13
	[I.5] Avería de origen físico o lógico	4	4	14
Administrativos	[A.30] Ingeniería social (picaresca)	4	4	15
Médicos generales	[A.30] Ingeniería social (picaresca)	4	4	15
Odontólogos	[A.30] Ingeniería social (picaresca)	4	4	15
Usuarios	[A.30] Ingeniería social (picaresca)	4	4	15
Proveedores	[A.30] Ingeniería social (picaresca)	4	4	15
***R:** Riesgo, **P**: Probabilidad, **I**: Impacto*				

Fuente: Los Autores

4. PLAN DE TRATAMIENTO DE RIESGOS CON BASE EN LOS CONTROLES DE LA NORMA NTC-ISO-IEC 27001:2013

Esta actividad tiene como fin relacionar los controles que se deben aplicar a cada riesgo, calificando su eficiencia frente a las amenazas que pretenden mitigar.

- Identificación de los controles.

4.1 IDENTIFICACIÓN DE LOS CONTROLES

En esta etapa se busca identificar los controles a implementar en los activos ya analizados. En el cuadro 15, se hace la identificación de los controles y se listan los activos a los cuales se les aplicarán dichos controles.

Cuadro 15. Identificación de controles

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Aplicaciones			
Heon	[E.21] Errores de mantenimiento / actualización de programas (software)	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
		A.12.1.4	Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
		A.12.3.1	Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
	[A.5] Suplantación de la identidad del usuario	A.9.1.1	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
		A.9.4.2	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
Sistema operativo	[I.5] Avería de origen físico o lógico	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.1] Errores de los usuarios	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
		A.9.4.2	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on
	[E.8] Difusión de software dañino	A.12.2.1	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
	[E.21] Errores de mantenimiento / actualización de programas (software)	A.9.4.4	El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.
		A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Aplicaciones			
Ofimática	[E.1] Errores de los usuarios	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
	[E.21] Errores de mantenimiento / actualización de programas (software)	A.12.3.1	Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
		A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Antivirus	[E.8] Difusión de software dañino	A.12.2.1	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
	[E.21] Errores de mantenimiento / actualización de programas (software)	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
		A.12.4.1	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
		A.12.4.2	Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
		A.12.4.3	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Aplicaciones			
Navegador web	[E.1] Errores de los usuarios	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
	[E.8] Difusión de software dañino	A.12.2.1	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
		A.12.1.4	Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
	[I.5] Avería de origen físico o lógico	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[I.8] Fallo de servicios de comunicaciones	A.13.1.2	Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.
		A.13.2.1	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Equipos			
Servidor de Correo	[E.1] Errores de los usuarios	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
	[E.8] Difusión de software dañino	A.12.2.1	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
	[I.5] Avería de origen físico o lógico	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.21] Errores de mantenimiento / actualización de programas (software)	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
	[I.8] Fallo de servicios de comunicaciones	A.13.2.1	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
	[A.6] Abuso de privilegios de acceso	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	[A.7] Uso no previsto	A.7.2.1	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Equipos			
Equipos de computo	[I.5] Avería de origen físico o lógico	A.8.1.1	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
		A.8.1.3	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
		A.8.2.3	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.24] Caída del sistema por agotamiento de recursos	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[A.6] Abuso de privilegios de acceso	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	[A.7] Uso no previsto	A.7.2.1	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Equipos			
Servidor Windows	[I.5] Avería de origen físico o lógico	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.12.4.1	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
	[E.2] Errores del administrador del sistema / de la seguridad	A.12.4.3	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.
		A.9.2.5	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A.12.3.1	Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[A.11] Acceso no autorizado	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Equipos			
Servidor Linux	[I.5] Avería de origen físico o lógico	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.12.4.1	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
	[E.2] Errores del administrador del sistema / de la seguridad	A.12.4.3	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.
		A.9.2.5	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.12.3.1	Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
	[A.11] Acceso no autorizado	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Equipos			
Impresoras	[I.5] Avería de origen físico o lógico	A.8.1.1	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
		A.8.1.3	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
		A.8.2.3	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A.9.2.5	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
Routers	[I.5] Avería de origen físico o lógico	A.9.1.2	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[A.11] Acceso no autorizado	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Equipos			
Switches	[I.5] Avería de origen físico o lógico	A.8.2.3	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[A.11] Acceso no autorizado	A.9.1.2	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.
		A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
Equipos Biomédicos	[I.5] Avería de origen físico o lógico	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Escáneres	[I.5] Avería de origen físico o lógico	A.8.1.1	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
		A.8.1.3	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
		A.8.2.3	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Equipos			
Módems	[I.5] Avería de origen físico o lógico	A.9.1.2	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Discos duros	[I.5] Avería de origen físico o lógico	A.8.2.3	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.*] Errores y fallos no intencionados	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Memorias USB	[I.5] Avería de origen físico o lógico	A.8.2.3	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Redes/ Comunicaciones			
Red LAN	[A.11] Acceso no autorizado	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	[I.8] Fallo de servicios de comunicaciones	A.13.1.1	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
		A.13.2.1	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
Red WIFI	[I.8] Fallo de servicios de comunicaciones	A.13.1.1	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
		A.13.2.1	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
Internet	[I.8] Fallo de servicios de comunicaciones	A.13.1.3	Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.
		A.13.2.1	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
Red Telefónica	[I.8] Fallo de servicios de comunicaciones	A.13.2.1	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
	[I.5] Avería de origen físico o lógico	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Infraestructura			
Plataformas móviles	[I.8] Fallo de servicios de comunicaciones	A.8.2.3	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
		A.13.2.1	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
	[I.5] Avería de origen físico o lógico	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Administrativos	[A.30] Ingeniería social (picaresca)	A.7.1.1	Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
		A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la Organización pertinentes para su cargo.
Médicos Generales	[A.30] Ingeniería social (picaresca)	A.7.1.1	Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
		A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la Organización pertinentes para su cargo.
Odontólogos	[A.30] Ingeniería social (picaresca)	A.7.1.1	Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
		A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la Organización pertinentes para su cargo.

Cuadro 15. (Continuación)

Activos	Riesgo/Amenaza	N°. Control ISO 270001:2013	Descripción del control a aplicar
Personal			
Usuarios	[A.30] Ingeniería social (picaresca)	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la Organización pertinentes para su cargo.
Proveedores	[A.30] Ingeniería social (picaresca)	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la Organización pertinentes para su cargo.
		A.15.1.1	Política de seguridad de la información para suministradores: Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.

Fuente: Los Autores

4.2 PLAN DE TRATAMIENTO DE RIESGOS

Después de analizar, cuantificar y valorar los riesgos según el impacto que tienen sobre los activos, se seleccionan las medidas más adecuadas para tratar los riesgos, con el fin de poder cambiar el riesgo. Se especifican aquellas actividades que tienen como objetivo detallar las actividades que se van a realizar a cada uno de los controles. Este plan debe ser aprobado por parte de la alta directiva ya que esto conlleva la destinación de recursos para alcanzar un estado manejable de los riesgos. En el cuadro 16, plan de tratamiento de los riesgos se describen las actividades a realizar con el fin de evitar incidentes que atenten contra la seguridad de la información.

Cuadro 16. Plan de tratamiento de los riesgos

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Aplicaciones			
Heon	[E.21]	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información en especial en el acceso al aplicativo HEON
		A.12.1.4	Separar los entornos de desarrollo y pruebas.
		A.12.3.1	Realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema de copias de respaldo
	[A.5]	A.9.1.1	Establecer, documentar y revisar una política de control de acceso al aplicativo dadas por el líder de TIC
		A.9.4.2	Implementación de contraseñas y tarjetas de identidad (smartcard), para el acceso al aplicativo y a los diferentes sitios que dispongan de seguridad física y lógica para su manipulación.
Sistema operativo	[I.5]	A.11.2.4	Realizar actualizaciones y mantenimiento preventivos de los sistemas operativos según directriz del departamento de sistemas
	[E.1]	A.7.2.2	Realizar actividades de concientización, Escritorio limpio y protector de pantalla formativo.
		A.9.4.2	Implementación de contraseñas de acuerdo al rol establecido por la empresa, de acuerdo a las funciones dadas por el empleador
	[E.8]	A.12.2.1	Realizar controles de detección, de prevención y de recuperación; Así como formación en cuanto al tratamiento de códigos maliciosos.
	[E.21]	A.9.4.4	Restringir el uso de aplicativos sin la respectiva evaluación.
		A.12.5.1	Establecer procedimientos de instalación de software en sistemas operativos.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Aplicaciones			
Ofimática	[E.1]	A.7.2.2	Realizar actividades de concientización, Escritorio limpio y protector de pantalla formativo.
	[E.21]	A.12.3.1	Realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema de copias de respaldo
		A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información
Antivirus	[E.8]	A.12.2.1	Realizar controles de detección, de prevención y de recuperación; Así como formación en cuanto al tratamiento de códigos maliciosos.
	[E.21]	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información
		A.12.4.1	Llevar registros periódicos de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
		A.12.4.2	Se establecen las autorizaciones asignadas para controlar el acceso al sistema según la política aplicable
		A.12.4.3	Llevar un registro de las actividades del administrador y operador del sistema, en este caso el líder de TIC.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Aplicaciones			
Navegador web	[E.1]	A.7.2.2	Realizar actividades de concientización, Escritorio limpio y protector de pantalla formativo.
	[E.8]	A.12.2.1	Realizar controles de detección, de prevención y de recuperación; Así como formación en cuanto al tratamiento de códigos maliciosos.
		A.12.1.4	Separar los entornos de desarrollo y pruebas
	[I.5]	A.11.2.4	Realizar actualizaciones y mantenimiento preventivos de los sistemas operativos según directriz del departamento de sistemas
	[I.8]	A.13.1.2	Realizar el acuerdo SLA entre una empresa de servicios y su cliente, definiendo, el servicio y los compromisos de calidad.
		A.13.2.1	Diseñar políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Equipos			
Servidor de Correo	[E.1]	A.7.2.2	Realizar actividades de concientización, Escritorio limpio y protector de pantalla formativo.
	[E.8]	A.12.2.1	Realizar controles de detección, de prevención y de recuperación; Así como formación en cuanto al tratamiento de códigos maliciosos.
	[I.5]	A.11.2.4	Realizar actualizaciones y mantenimiento preventivos de los sistemas operativos según directriz del departamento de sistemas
	[E.21]	A.12.1.2	Mantener una ruta de las actualizaciones del software
	[I.8]	A.13.2.1	Diseñar políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. Entre ellas el uso de correo para el desempeño de las funciones asignadas y prohibir el uso para fines personales, identificar los tipos de correo permitidos
	[A.6]	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Estos permisos solo pueden ser dados por el líder de TIC de la empresa ya que cuenta con los permisos necesarios
	[A.7]	A.7.2.1	La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Equipos			
Equipos de computo	[I.5]	A.8.1.1	Todos los activos relacionados con el servidor de copias deben estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
		A.8.1.3	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
		A.8.2.3	Desarrollar procesos para la manipulación de información, con el fin de organizarla de manera administrativa y asistencial en cada una de las sedes de la empresa.
		A.11.2.4	Realizar actualizaciones y mantenimiento preventivos de los sistemas operativos según directriz del departamento de sistemas
	[E.23]	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.24]	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[A.6]	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Estos permisos solo pueden ser dados por el líder de TIC de la empresa ya que cuenta con los permisos necesarios
	[A.7]	A.7.2.1	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Equipos			
Servidor Windows	[I.5]	A.11.2.4	Realizar actualizaciones y mantenimiento preventivos de los sistemas operativos según directriz del departamento de sistemas
		A.12.4.1	Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del servidor
	[E.2]	A.12.4.3	Las actividades del administrador y operador del sistema deben ser registradas y estos deben ser protegidos y revisados periódicamente
		A.9.2.5	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.
	[E.23]	A.12.3.1	Se deben hacer copias de seguridad de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[A.11]	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Estos permisos solo pueden ser dados por el líder de TIC de la empresa ya que cuenta con los permisos necesarios

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Equipos			
Servidor Linux	[I.5]	A.11.2.4	Realizar actualizaciones y mantenimiento preventivos de los sistemas operativos según directriz del departamento de sistemas
		A.12.4.1	Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del servidor
	[E.2]	A.12.4.3	Las actividades del administrador y operador del sistema deben ser registradas y estos deben ser protegidos y revisados periódicamente
		A.9.2.5	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.
	[E.23]	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.12.3.1	Se deben hacer copias de seguridad de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
	[A.11]	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Estos permisos solo pueden ser dados por el líder de TIC de la empresa ya que cuenta con los permisos necesarios

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Equipos			
Impresoras	[I.5]	A.8.1.1	Se deben identificar los activos relacionados con el servidor de copias de respaldo que están asociados con el manejo de información, además se debe elaborar y mantener actualizado el inventario de los mismos.
		A.8.1.3	La documentación generada en los dispositivos debe ser controlada y vigilada para evitar perdida de información confidencial de la empresa.
		A.8.2.3	Desarrollar procesos para la manipulación de información, con el fin de organizarla de manera administrativa y asistencial en cada una de las sedes de la empresa.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.23]	A.9.2.5	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.
Routers	[I.5]	A.9.1.2	Solo se debe permitir acceso a la red y a sus servicios de acuerdo al rol de la persona direccionada, capacitada y con los permisos dados por parte del líder de TIC
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[A.11]	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Entre ellos el administrador del servidor

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Equipos			
Switches	[I.5]	A.8.2.3	Desarrollar procesos para la manipulación de información, con el fin de organizarla de manera administrativa y asistencial en cada una de las sedes de la empresa.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[A.11]	A.9.1.2	Solo se debe permitir acceso a la red y a sus servicios de acuerdo al rol de la persona direccionada, capacitada y con los permisos dados por parte del líder de TIC
		A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Estos permisos solo pueden ser dados por el líder de TIC de la empresa ya que cuenta con los permisos necesarios
Equipos Biomédicos	[I.5]	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Escáneres	[I.5]	A.8.1.1	Se deben identificar los activos relacionados con el servidor de copias de respaldo que están asociados con el manejo de información, además se debe elaborar y mantener actualizado el inventario de los mismos.
		A.8.1.3	La documentación generada en los dispositivos debe ser controlada y vigilada para evitar perdida de información confidencial de la empresa.
		A.8.2.3	Desarrollar procesos para la manipulación de información, con el fin de organizarla de manera administrativa y asistencial en cada una de las sedes de la empresa.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Equipos			
Modems	[I.5]	A.9.1.2	Solo se debe permitir acceso a la red y a sus servicios de acuerdo al rol de la persona.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Discos duros	[I.5]	A.8.2.3	Desarrollar procesos para la manipulación de documentación, con el fin de organizarla de manera administrativa y asistencial en cada una de las sedes de la empresa.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	[E.*]	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Memorias Usb	[I.5]	A.8.2.3	Desarrollar procesos para la manipulación de información, con el fin de organizarla de manera administrativa y asistencial en cada una de las sedes de la empresa.
		A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Redes/ Comunicaciones			
Red LAN	[A.11]	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Estos permisos solo pueden ser dados por el líder de TIC de la empresa ya que cuenta con los permisos necesarios
	[I.8]	A.13.1.1	Las redes se deben gestionar y controlar buscando proteger la información que viaja a través de ellas.
		A.13.2.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones ya que la única segmentación existente es la que apunta a Heon y la de la Red Pública.
Red WIFI	[I.8]	A.13.1.1	Las redes se deben gestionar y controlar buscando proteger la información que viaja a través de ellas.
		A.13.2.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones ya que la única segmentación existente es la que apunta a Heon y la de la Red Pública.
Internet	[I.8]	A.13.1.3	Se debe separar de las redes los grupos, usuarios y servicios de información.
		A.13.2.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones ya que la única segmentación existente es la que apunta a Heon y la de la Red Pública.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Redes/ Comunicaciones			
Red Telefónica	[I.8]	A.13.2.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones ya que la única segmentación existente es la que apunta a Heon y la de la Red Pública.
	[I.5]	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Infraestructura			
Plataformas móviles	[I.8]	A.8.2.3	Desarrollar procesos para la manipulación de información, con el fin de organizarla de manera administrativa y asistencial en cada una de las sedes de la empresa.
		A.13.2.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones ya que la única segmentación existente es la que apunta a Heon y la de la Red Pública.
	[I.5]	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Personal			
Administrativos	[A.30]	A.7.1.1	Se deben verificar los antecedentes de todos los candidatos a un empleo y estas deben estar de acuerdo a las leyes vigentes. La creación de usuarios por parte del líder de TIC es tipo estándar para no con el fin de no tener privilegios en el sistema.
		A.7.2.2	Todos los empleados de la organización y los proveedores deben recibir educación en la toma de conciencia, en las políticas de seguridad y procedimientos de seguridad de la información.

Cuadro 16. (Continuación)

Activos	Id. del riesgo	N°. Control ISO 270001:2013	Actividad de tratamiento
Personal			
Médicos Generales	[A.30]	A.7.1.1	Se deben verificar los antecedentes de todos los candidatos a un empleo y estas deben estar de acuerdo a las leyes vigentes. La creación de usuarios por parte del líder de TIC es tipo estándar para no con el fin de no tener privilegios en el sistema.
		A.7.2.2	Todos los empleados de la organización y los proveedores deben recibir educación en la toma de conciencia, en las políticas de seguridad y procedimientos de seguridad de la información.
Odontólogos	[A.30]	A.7.1.1	Se deben verificar los antecedentes de todos los candidatos a un empleo y estas deben estar de acuerdo a las leyes vigentes. La creación de usuarios por parte del líder de TIC es tipo estándar para no con el fin de no tener privilegios en el sistema.
		A.7.2.2	Todos los empleados de la organización y los proveedores deben recibir educación en la toma de conciencia, en las políticas de seguridad y procedimientos de seguridad de la información.
Usuarios	[A.30]	A.7.2.2	Todos los empleados de la organización y los proveedores deben recibir educación en la toma de conciencia, en las políticas de seguridad y procedimientos de seguridad de la información.
Proveedores	[A.30]	A.7.2.2	Todos los empleados de la organización y los proveedores deben recibir educación en la toma de conciencia, en las políticas de seguridad y procedimientos de seguridad de la información.
		A.15.1.1	Con el objetivo de mitigar los riesgos se deben establecer y acordar todos los requisitos de seguridad de la información con los proveedores

Fuente: Los Autores

5. ALCANCE Y POLÍTICA DE SEGURIDAD

5.1 ALCANCE DE LA POLÍTICA GENERAL PARA CORVESALUD

El alcance permite determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información de la entidad[22].

La política general tiene como alcance a toda la entidad, sus funcionarios, contratistas, terceros vinculados a la entidad CORVESALUD IPS y la ciudadanía en general. Su aplicabilidad engloba a todas las personas que tienen relaciones de tipo comercial y laboral con la entidad, por lo cual esta es de estricto cumplimiento.

5.2 POLÍTICA GENERAL DEL SGSI PARA CORVESALUD IPS

La política de alto nivel o política general, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI. Partiendo de esta premisa la entidad genera su política teniendo en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Dirección. [23]

Esta política debe ser informada, socializada y promovida de manera estricta a todos los entes vinculados a la entidad, a continuación, se redacta la política general del sistema de gestión de seguridad de la información para la empresa CORVESALUD IPS.

La junta directiva de CORVESALUD IPS, entiende que la entidad debe tener una adecuada gestión de la información y se compromete con la implementación de un sistema de gestión de seguridad de la información buscando establecer un clima confiable en el ejercicio de deberes con el estado y los usuarios, todo enmarcado en el estricto cumplimiento de las leyes, en concordancia con la misión y visión de la entidad.

Para CORVESALUD IPS, la protección de la información tiene como fin primordial minimizar el impacto generado sobre los activos de información, por los riesgos identificados de manera sistemática con el propósito de mantener la integridad,

[22] ICONTEC, NTC-ISO-IEC 27001, 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Pág. 2

[23] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Elaboración de la política general de seguridad y privacidad de la información. [En Línea]. 2017. [Citado el 24.Septiembre.2017]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

Con base en lo anterior, esta política aplica a CORVESALUD IPS, como se defina en el alcance, sus funcionarios, terceros, proveedores, usuarios y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de la toma de decisiones alrededor del SGSI, estarán determinadas por las siguientes premisas:

- *Minimizar el riesgo en las operaciones de la entidad.*
- *Cumplir con los principios de seguridad.*
- *Mantener la confianza de sus clientes, socios y empleados.*
- *Apoyar la innovación tecnológica.*
- *Proteger los activos tecnológicos de la entidad.*
- *Establecer las políticas y procedimientos en materia de seguridad de la información.*
- *Garantizar la continuidad del negocio.*
- *Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de CORVESALUD IPS.*
- *CORVESALUD IPS ha decidido definir, implementar, operar y mejorar de forma continua un sistema de gestión de seguridad de la información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.*

5.3 ALCANCE Y POLÍTICA PARA EL SERVIDOR DE COPIAS DE RESPALDO

Este alcance abarca solo el proceso de copias de respaldo de CORVESALUD IPS, que involucra la gestión de la infraestructura, plataforma de procesamiento de información, gestión de aplicaciones, gestión de Incidentes, requerimientos y gestión de cambios de TI, además de los responsables y usuarios del sistema de información. Se establece una política de seguridad general para el proceso de copias de respaldo en la entidad, garantizando así que la información que se esté manipulando y almacenando de la mejor manera, evitando daños y pérdidas de la misma.

5.4 POLÍTICA DEL SERVIDOR DE COPIAS DE RESPALDO

La política de Seguridad de la información para el proceso de copias de respaldo de la organización Corvesalud IPS, corresponde a la declaración general que representa la posición de la *Alta Directiva* de la entidad con relación a la seguridad de la información en este proceso. La norma ISO/IEC 27001:2013 en su apartado 5.2 Política, indica que la alta dirección debe establecer una política de la seguridad de la información que sea adecuada al propósito de la organización, que incluya los objetivos de seguridad de la información, los requerimientos normativos vigentes relacionados con seguridad de la información y el compromiso de la mejora continua.[24]

La siguiente es la política general del sistema de seguridad de la información que se definió para el sistema de copias de respaldo.

CORVESALUD IPS, identifica la información como uno de sus principales activos, por esta razón entiende y prioriza la protección de la misma, garantizando la disponibilidad, integridad y la búsqueda de la confidencialidad implementando varios controles, que puedan garantizar la confianza en el proceso de copias de respaldo de la entidad, haciendo uso de un sistema de gestión de seguridad de la información en el mismo. Esta política y las que se desprenden de los distintos activos deben ser revisadas y actualizadas anualmente con el fin de garantizar la continuidad del negocio.

Aplicabilidad de la Política del SGSI. Esta política aplica al sistema de copias de respaldo, sus colaboradores, proveedores, terceros y demás partes interesadas.

5.5 OBJETIVOS DE LA POLÍTICA DEL SERVIDOR DE COPIAS DE RESPALDO

- Mejorar el nivel de confianza de la entidad en el servidor de copias de respaldo de la misma por medio de controles y políticas.

- Respaldar el acceso a la información del servidor de copias de respaldo de la entidad, de acuerdo con los niveles organizacionales, criterios de la entidad, la normatividad aplicable y las partes interesadas.

- Preservar que la información que posee el servidor de copias de respaldo de la organización esté disponible para los procesos autorizados que así lo requieran.

[24] ICONTEC, NTC-ISO-IEC 27001, 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Pág. 3

- Mantener la integridad y disponibilidad de la información, teniendo en cuenta los requisitos de seguridad aplicables, los resultados de valoración de riesgos y el tratamiento de los mismos.

5.6 POLÍTICAS GENERALES

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con CORVESALUD IPS sobre la importancia, sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.[25]
Basados en lo anterior se proponen políticas generales soportados en la norma ISO 27001:2013, que permitirán tener mayor confianza en el proceso del servidor de copias de respaldo.

Objetivo de control *A.5. Políticas de Seguridad de la Información.*
Las siguientes políticas describen la importancia de la orientación y el soporte que debe dar la alta dirección para la seguridad de la información.

- La alta gerencia debe dirigir, aprobar, publicar, modificar, actualizar y comunicar las políticas de seguridad de la entidad, que acciones seguir en cuanto al servidor de copias de respaldo de la entidad.

- Se debe designar un encargado de la seguridad de la información, que presente estrategias, lidere y audite el sistema de seguridad de la información de la entidad, en especial en el servidor de copias de respaldo.

- Los usuarios del proceso del servidor de copias deben conocer y acatar las políticas, se les debe brindar formación en cuanto a la importancia que tienen en el proceso, estas deben ser presentadas por medio escrito y deben ser leídas y firmadas como parte de la responsabilidad con el proceso de seguridad.

- Cuando sucedan anomalías estas deben ser reportadas al responsable de TIC, estas deben ir por escrito especificando la falla y permitiendo llevar un control que permita la mejora continua.

[25] PRESIDENCIA DE LA REPÚBLICA. Manual de la política de seguridad para las tecnologías de la información y las comunicaciones – TICS. [En Línea]. 2017. [Citado el 24.Septiembre.2017]. Disponible en internet: http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf>

5.7 POLÍTICAS ORGANIZACIONALES

Objetivo de control *A.6. Organización de la Seguridad de la Información.*

Las siguientes políticas describen las responsabilidades y roles de los usuarios vinculados al servidor de copias de respaldo de la entidad.

- *La Alta dirección* debe comprometerse con la implementación, establecimiento, operación, monitorización, mantenimiento, revisión y mejora del Sistema de Seguridad de la Información.

- El *Coordinador de la seguridad informátic*a es el líder del proceso de seguridad de la información, por tal motivo planea, organiza y promueve todas las actividades que están vinculadas a ese proceso.

- El *Administrador* tiene la responsabilidad de asignar las responsabilidades y privilegios en el sistema de información, basado en las políticas de seguridad de la entidad.

- Los *usuarios* que son los que hacen uso del servidor de copias, deben respetar las políticas de seguridad de la información del servidor, además deben reportar cualquier anomalía en el mismo al encargado de TIC, para tomar las acciones pertinentes.

- Se deben mantener vínculos con autoridades y grupos especializados en seguridad de la información que retroalimenten el sistema de seguridad de la información y brinden apoyo en caso de cualquier emergencia.

5.8 POLÍTICAS DE RECURSOS HUMANOS

Objetivo de control *A.7. Seguridad de los Recursos Humanos.*

Las políticas de recursos humanos están enfocadas a que los empleados y contratistas comprendan sus responsabilidades y sean idóneos en su labor.

- Las personas que sean vinculadas a la empresa y tengan responsabilidad con el servidor de copias de respaldo deben ser seleccionadas teniendo en cuenta sus antecedentes y referencias de acuerdo a las leyes existentes, además dentro de sus contratos deben estar expuestos los delitos informáticos para que conozcan sus responsabilidades con la entidad desde su vinculación.

- Se debe capacitar al personal nuevo en cuanto a las políticas de seguridad que rigen el servidor de copias de respaldo, los delitos informáticos y los procesos de seguridad de la información.

5.9 POLÍTICAS DE GESTION DE ACTIVOS

Objetivo de control *A.8. Gestión de Activos.*

Las siguientes políticas describen las responsabilidades en cuanto al uso de los activos de información.

- Se deben mantener actualizado el inventario de activos en el proceso de copias de respaldo de la entidad, las reglas del uso adecuado de este deben estar documentados, identificadas e implementadas.

- Cuando se dé por terminado el contrato con el empleado, este tiene la responsabilidad de devolver todos los activos de la organización que se encuentren a su cargo.

- Ningún usuario del sistema podrá acceder al servidor de copias de respaldo con el usuario y contraseña de otro, de conocerse una anomalía; esta debe ser informada de manera urgente al jefe inmediato para realizar las respectivas acciones.

5.10 POLÍTICAS DE GESTIÓN DE ACCESO DE USUARIOS

Objetivo de control *A.9. Control de Acceso.*

A continuación, se describen las políticas para la gestión de acceso a los activos del servidor de copias de respaldo.

- El responsable de la seguridad de la información debe establecer, documentar y revisar una política de control de acceso con base en las necesidades del servidor de copias de respaldo.

- Solo se debe permitir el acceso a la red a los usuarios que hayan sido autorizados para realizar esta actividad.

- Los permisos de acceso al servidor de copias deben ser restringidos, controlados en cuanto a los derechos privilegiados de uso. Estos deben ser revisados periódicamente para evitar alguna filtración no deseada.

- Se deben restringir y controlar el uso de utilidades de software que puedan anular el sistema, así como el acceso a códigos fuentes de los programas que están en el servidor de copias de respaldo.

5.11 POLÍTICA DE CRIPTOGRAFÍA

Objetivo de control *A.10. Criptografía*

A continuación, se listan las políticas referentes al uso de controles criptográficos, asociados al servidor de copias de la entidad.

- El área de sistemas definirá los mecanismos criptográficos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en el servidor de copias de respaldo.

- Se deben implementar y evaluar los procesos de uso y asignación de claves, recuperación de la información, en caso de pérdida o daño de las claves durante su tiempo de vida.

5.12 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo de control *A.11. Seguridad Física y del Entorno*

Las siguientes son las políticas referentes a la seguridad física y del entorno del servidor de copias de respaldo.

- Los equipos deben tener un mantenimiento, correctivo, predictivo y preventivo periódicamente con el fin de evitar la pérdida de estos y garantizar la disponibilidad e integridad continúas.

- Se debe verificar que todos los equipos estén protegidos contra fallos de suministro eléctrico y estar blindados contra cualquier amenaza que interrumpa su funcionamiento.

5.13 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

Objetivo de control *A.12. Seguridad de Operaciones*

Las siguientes políticas destacan los lineamientos para la seguridad de las operaciones sobre el servidor de copias de respaldo de la entidad.

- El encargado de TIC deberá asignar las funciones específicas a los administradores y usuarios del servidor de copias, así como velar por la aplicabilidad adecuada de los controles de seguridad de la información sobre el activo.

- Se debe establecer controles sobre las copias de respaldo del servidor, proporcionando los recursos necesarios, estableciendo los procedimientos y

mecanismos para la realización de las actividades de este. Así como la realización de pruebas en cuanto a la integridad de las copias.

- Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos; en especial en el servidor de copias de respaldo.

- Se deben mantener actualizados y parchados los programas residentes en el servidor de copias, además de realizar revisiones periódicas sobre su funcionamiento, acceso y actividades de los mismos.

- Se deben registrar y llevar control sobre las actividades del administrador del sistema, con el fin de llevar una auditoria sobre el uso correcto del servidor y evitar posibles bloqueos o fuga de información a futuro.

5.14 POLÍTICAS SOBRE LA SEGURIDAD EN LAS COMUNICACIONES

Objetivo de control *A.13. Seguridad de Operaciones.*

En cuanto a la seguridad de comunicaciones a continuación se listan las políticas a tener en cuenta.

- El encargado de TIC debe establecer mecanismos de control que permitan mantener activo el servicio de las redes, así como contar con los controles necesarios de seguridad de la red con el fin de evitar la caída de la misma o alguna intrusión inesperada.

- El administrador de la red debe segmentarla por dominios, grupos de servicios y usuarios, así como llevar control del acceso a la misma de todos los dispositivos y su respectivo funcionamiento.

- Se deben implementar procedimientos que permitan controlar la transferencia de datos desde el servidor de copias y la red.

5.15 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Objetivo de control *A.14. Adquisición, desarrollo y mantenimiento de sistemas*

Las siguientes son las políticas relacionadas con la adquisición, desarrollo y mantenimiento de los sistemas en el proceso de copias de respaldo de la entidad.

- El departamento de sistemas definirá los requisitos para los nuevos sistemas de información o para las mejoras de los existentes.

- Se debe asegurar que el software adquirido por la entidad cumpla con los estándares de seguridad y calidad, además deben ser sometidos a pruebas de aceptación por parte de la entidad.

- Los datos de pruebas deben ser seleccionados, protegidos y controlados cuidadosamente.

- Se debe definir los requerimientos de seguridad en el servidor de copias, teniendo en cuenta aspectos como el control de acceso, autenticación, arquitectura de aplicaciones entre otros.

5.16 POLÍTICAS DE LAS RELACIONES CON LOS PROVEEDORES

Objetivo de control *A.15. Protección de los Activos Accesibles a los Proveedores*

Las siguientes son las políticas proporcionan los lineamientos en cuanto a la relación de la entidad con los proveedores.

- Es necesario establecer controles debidamente documentados entre la entidad y los proveedores, que estén asociados al servidor de copias de respaldo, con el objetivo de asegurar el acceso a los servicios provistos por el mismo.

- Se debe garantizar el conocimiento por parte de los proveedores de las políticas, controles y procedimientos de seguridad de la información.

- Se debe capacitar a los proveedores en cuanto a las vulnerabilidades a las que están expuestos en cuanto a la fuga de información vital de la empresa, las posibles consecuencias de ser víctimas de ingeniería social y el impacto que esto tendría en la entidad.

6. PLAN DE IMPLEMENTACIÓN

Se establece un plan de implementación de seguridad de la información para el proceso de copias de respaldo en la empresa Corvesalud IPS.

Este proceso consiste en definir un orden al momento de poner en funcionamiento el sistema de seguridad de la información de la siguiente manera.

- Dar a conocer a la alta directiva de la empresa el Sistema diseñado con el fin de ilustrar el estado actual de la empresa en cuanto al proceso de copias de respaldo actual y a su vez exponer los beneficios que trae implementar este sistema de mejoramiento del proceso.

- Obtener la aprobación de recursos económicos por parte de la alta directiva con el fin de adquirir mejores innovaciones tecnológicas que permitan un mejor desarrollo del SGSI.

- Establecer el grupo de trabajo del área de sistemas enfocado en velar y responder que el proceso sea implementado de la mejor manera.

- Aprobado la implementación del sistema de seguridad en el proceso de copias de respaldo, se crean campañas de concientización para que el personal de la empresa sea capaz de analizar y determinar la importancia de proteger la información en las diferentes áreas de la empresa.

- Dar a conocer al personal las políticas de seguridad establecidas para el proceso y verificar que se dé un óptimo cumplimiento de las mismas.

- Realizar la evaluación y el tratamiento de los riesgos cada semestre, para obtener una visión integral de los peligros sobre la información de la organización de manera permanente.

- Diseñar un plan de seguimiento, en el cual se deben incluir las recomendaciones realizadas anteriormente.

- Redactar la declaración de aplicabilidad la cual enumera los controles del anexo A de la NTC-ISO-IEC 27001:2013, definiendo:

  - Cuales son aplicables y cuáles no.
  - El motivo de la decisión.
  - Los objetivos que se logrará.
  - Como se implementarán dichos controles.

- Redactar plan de tratamiento de los riesgos que permitan definir cómo se van a implementar los controles.

- Establecer procedimientos de control de cambio, que permitan asegurar la continuidad del negocio.

- Supervisar el sistema de seguridad de la información en el proceso de copias de respaldo, verificando si los resultados obtenidos cumplen con lo establecido en los objetivos, de lo contrario es necesario aplicar medidas correctivas y preventivas.

- La alta dirección debe realizar periódicamente el sistema de seguridad de la información en el proceso de copias de respaldo, para saber si se está cumpliendo con los objetivos propuestos.

- Diseñar medidas correctivas y preventivas que se apliquen sistemáticamente, las cuales tiendan a identificar la raíz del problema, darle solución y aplicar su respectivo control.

7. PLAN DE CONCIENCIACIÓN

Cuando en una organización se implementa un sistema de gestión de seguridad de la información, esta debe preguntarse si el personal está preparado y concienciado para realizarlo y mantenerlo. De ahí surge la necesidad de crear el plan de concienciación el cual tiene como objetivo sensibilizar, formar e incentivar las buenas prácticas de seguridad de la información en la entidad.

Objetivos:

- Lograr que todos los miembros de CORVESALUD IPS, entiendan, acaten y se comprometan con todos los aspectos relacionados con el sistema de gestión de seguridad de la información.

- Crear una cultura respecto al tema de la integridad, confidencialidad y disponibilidad de la información en donde todos los miembros de la entidad se conviertan en gestores de esa cultura y le den importancia al tratamiento adecuado de la información.

- Crear conciencia en todos los miembros de la entidad sobre los riesgos a los que están expuestos ellos y los activos de información de la entidad.

Actividades:

- Realizar una encuesta para analizar los problemas y necesidades de la entidad.

- El plan de concientización va dirigido a todos los miembros de la entidad esto es: a sus funcionarios, terceros, aprendices, practicantes, proveedores y usuarios.

- Crear un eslogan y una mascota con la cual los participantes se puedan identificar.

- Sensibilización sobre las leyes LEY 1273 DE 2009 “de la protección de la información y de los datos” y LEY ESTATUTARIA 1581 DE 2012 “disposiciones generales para la protección de datos personales”.

- Talleres didácticos sobre el uso de contraseñas, protección contra virus, el respeto y apropiación de las políticas de seguridad, uso adecuado del correo electrónico e internet, backup de los datos, pasos a seguir al presentarse incidentes, ingeniería social, seguridad de dispositivos USB, medidas de seguridad y tratamiento de información sensible, software permitido o no permitido, seguridad de equipos.

- Realización de encuestas de evaluación y satisfacción para poder llevar un control del programa de concienciación.

- Estas actividades deben ser repetidas de manera periódica por medio de simulacros y otras actividades que permitan fortalecer el conocimiento adquirido por los miembros de la entidad.

8. CONCLUSIONES

- El análisis de riesgos realizado a los activos del servidor de copias de respaldo, muestra las debilidades de ese sistema; la indiferencia a ese análisis hará que con el tiempo se pueda perder información importante de ese proceso y por ende la entidad pierda prestigio y confianza por parte de los usuarios.

- Los resultados obtenidos de este análisis ayudarán a la entidad a reconocer la importancia de implementar un sistema de gestión de la seguridad de la información, que permitan mitigar los riesgos a los que están expuestos los activos entre ellos el servidor de copias de respaldo, mientras que se pueda contratar personal especializado en la seguridad de la información.

- Se requiere implementar los controles que aún no existen y fortalecer los existentes, con el objetivo de asegurar la seguridad de la información en el servidor de copias de respaldo de la entidad y con ello garantizar que los cambios que se realizan en el proceso no afecten la operación ni la seguridad de la información de la entidad.

- No existen políticas de seguridad de la información enfocadas al proceso, por ende, es importante que éstas mismas sean definidas, implementadas y debidamente cumplidas por parte de todos los usuarios que dependan del proceso de copias de respaldo de la empresa.

9. RECOMENDACIONES

La entidad Corvesalud IPS, no posee un sistema de gestión de la seguridad de la información, se hace necesario delegar un oficial de seguridad que vele por la implementación de políticas y normas que propendan la protección de los activos de información, en el servidor de copias de respaldo de la entidad.

La alta gerencia debe involucrarse más en la implementación de las políticas de seguridad de la entidad, pues ellos tienen que ser los garantes e impulsadores de dicho proceso.

Se debe nombrar personas del grupo de TICS, los cuales deben encargarse de la seguridad de la información de la empresa, buscando prioridades en la continuidad y verificación de los procesos concernientes al proceso de copias de respaldo.

BIBLIOGRAFÍA

ADVISERA EXPERT SOLUTIONS LTD. Herramienta gratuita de análisis de brecha para ISO 27001 [En Línea]: [Citado 24, junio 2017]. Disponible en internet: <URL: https://advisera.com/27001academy/es/herramientas/herramienta-gratuita-analisis-de-brecha-para-iso-27001/

_____. Lista de verificación ISO 27001: 16 pasos para la implementación. [En línea]. Disponible En: https://advisera.com/27001academy/es/knowledgebase/lista-de-apoyo-para-implementacion-de-iso-27001/ . Citado el [14 de agosto del 2017].

CONGRESO DE COLOMBIA, Ley Estatutaria 1581 de 2012, [En línea]. Disponible En: http://www.sic.gov.co/drupal/sites/default/files/normatividad/Ley_1581_2012.pdf. Citado el [8 Julio 2017].

_____. Ley Estatutaria 1266 de 2008, [En línea]. Disponible En: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html. Citado el [8 Julio 2017].

CORVESALUD IPS. ¿Quiénes Somos? [En Línea] Bogotá, D.C.: [Citado 8, julio 2017]. Disponible en internet: <URL: http://www.corvesalud.com.co/quienes-somos/>

DECRETO 1377 DE 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

ICONTEC, GUIA TECNICA COLOMBIA GTC-ISO/IEC 27035, 2015. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Citado el [7 Julio 2017].

_____, NTC-ISO-IEC 27000, 2014. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario. Citado el [8 Junio 2017].

_____, NTC-ISO-IEC 27001, 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos, pág. 2.

_____, NTC-ISO-IEC 27001, 2013.Anexo A. En: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC, 2013, 13-24 p. (NTC-ISO/IEC 27001).

_____, NTC-ISO-IEC 27002, 2013. Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. En: Compendio Sistema de Gestión de la Seguridad de la Información. 2 ed. Bogotá, D.C. ICONTEC. Agosto 2015. ISBN Impreso: 978-958-8585-53-6.

ISO-IEC 27000: 2014. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario. [En Línea]: [Citado 13, junio 2017]. Disponible en internet: <URL: https://www.normasiso.net/wp-content/uploads/2016/10/iso-27000.pdf>

_____. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Capítulo Introducción. P. i. [En Línea]: [Citado 13, junio 2017]. Disponible en internet: <URL: https://www.normasiso.net/wp-content/uploads/2016/10/iso-27000.pdf>

LEY 100 DE 1993. “Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones” Preámbulo.

LEY 1438 DEL 19 DE ENERO DE 2011 SENADO. “Por medio de la cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones”. Artículo 1.

LEY ESTATUTARIA 1581 del 17 de octubre de 2012 “Por el cual se dictan disposiciones generales para la protección de los datos personales”.

MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, Proyectos de análisis de riegos. MAGERIT – Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1-Metodo [En Línea] Bogotá, D.C.: [Citado 8, julio 2017]. Disponible en internet: <URL: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WWDkIIg1_IU >

_____, Proyectos de análisis de riegos. MAGERIT – Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 2-Catalogo de Elementos, pág. 19, 52 [En Línea] Bogotá, D.C.: [Citado 8, julio 2017]. Disponible en internet: <URL: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WWDkIIg1_IU>

_____, Proyectos de análisis de riegos. MAGERIT – Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 3- Guía de Técnicas. [En Línea] Bogotá, D.C.: [Citado 8, julio 2017]. Disponible en internet: <URL: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WWDkIIg1_IU>

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Elaboración de la política general de seguridad y privacidad de la información. [[En Línea] Bogotá, D.C.: [Citado 24, septiembre 2017]. Disponible en internet: <URL: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Resolución Número 00002003 DE 2014. “Por la cual se definen los procedimientos y condiciones de inscripción de los Prestadores de Servicios de Salud y de habilitación de servicios de salud”

MINISTERIO DE LA PROTECCION SOCIAL.DECRETO NÚMERO 1011 DE 2006. “Por el cual se establece el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud”. Campo de aplicación.

PMG-SSI. ISO 27001 – ¿Cómo confeccionar un plan de concienciación sobre la Seguridad de la Información? [En Línea]: [Citado 12, octubre 2017]. Disponible en internet: <URL: http://www.pmg-ssi.com/2014/06/iso-27001-como-confeccionar-un-plan-de-concienciacion-sobre-la-seguridad-de-la-informacion/>

PRESIDENCIA DE LA REPÚBLICA. Manual de la política de seguridad para las tecnologías de la información y las comunicaciones – TICS. [En Línea]. 2017. [Citado el 24.Septiembre.2017]. Disponible en internet: http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf>

_____, Decreto 1377 de 2013, [En línea]. Disponible En: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf. Citado el [8 Julio 2017].

SUPERINTENDENCIA FINANCIERA DE COLOMBIA, Circular Externa 038, 2009.

_____, Circular Externa 052, 2007

ANEXOS

ANEXO 1.CUESTIONARIO ANALISIS DE BRECHA DE LA ENTIDAD

Esta encuesta permite evaluar el nivel de implementación de la ISO 27001 en tu organización; pasa saber si se está en un nivel inicial o si falta mucho para alcanzar un estado adecuado. Por favor selecciones sí o no dependiendo de la aplicabilidad del ítem.

Análisis de brecha		
Contexto de la organización	**S**	**N**
1. ¿La organización determina los fines del SGSI?		
2. ¿La organización determina las cuestiones internas y externas que son pertinentes para la finalidad de SGSI?		
3. ¿Determina la organización cómo las cuestiones internas y externas podrían influenciar en la capacidad del SGSI para conseguir los resultados previstos?		
4. ¿La organización determina las partes interesadas?		
5. ¿Existe la lista de todos los requisitos de las partes interesadas?		
6. ¿El alcance está documentado con los límites claramente definidos?		
7. ¿Han establecido, documentado, implementado, mantenido y mejorado continuamente un sistema de gestión de seguridad de información según los requisitos de la norma ISO 27001?		
Liderazgo y compromiso		
8. ¿Los objetivos generales del SGSI son compatibles con la dirección estratégica?		
9. ¿La dirección garantiza los recursos necesarios para el SGSI cuando sea necesario?		
10. ¿La dirección asegura que el SGSI logra sus resultados previstos?		

Anexo A. (Continuación)

Análisis de brecha		
Política		
11. ¿Existe una política de seguridad de la información con objetivos definidos o un marco para el establecimiento de objetivos?		
12. ¿La política de seguridad de información está documentada y es comunicada dentro de la empresa y a otras partes interesadas?		
13. ¿Están asignadas y comunicadas los roles, responsabilidades y autoridades para la seguridad de la información?		
Planificación		
14. ¿Las cuestiones internas y externas, así como los requisitos de las partes interesadas, son consideradas al abordar los riesgos y las oportunidades?		
15. ¿Hay un proceso documentado para identificar los riesgos de seguridad de la información, incluyendo los criterios de aceptación del riesgo y criterios de evaluación del riesgo?		
16. ¿Está documentado el proceso de tratamiento del riesgo, incluyendo las opciones de tratamiento del riesgo y cómo crear una declaración de aplicabilidad?		
17. ¿Los objetivos de seguridad de la información son establecidos en las funciones relevantes de la organización, medido en su práctica y coherente con la política de seguridad de la información?		
18. ¿Existe un plan, o conjunto de planes, para lograr los objetivos de seguridad de la información incluyendo responsabilidades, método de evaluación y tiempos para el plan?		
Soporte		
19. ¿Se proporcionan los recursos adecuados para todos los elementos del SGSI?		
20. ¿Es evaluada la competencia, y la capacitación donde sea necesario, para el personal que realiza tareas que puedan afectar a la seguridad de la información? ¿Los registros de competencias son mantenidos?		
21. ¿El personal es consciente de la política de seguridad de la información, de su papel y las consecuencias de no cumplir con las normas?		

Anexo A. (Continuación)

Análisis de brecha		
Soporte		
22. ¿Hay un proceso de comunicación relacionado con la seguridad de la información, incluyendo las responsabilidades, qué se comunica, a quién y cuándo?		
23. ¿La documentación del SGSI incluye la política de seguridad de la información, objetivos, el alcance del SGSI, los principales elementos y su interacción, documentos y registros de la norma ISO 27001 y aquellos identificados por la empresa?		
24. ¿Se asegura que existe un manejo de documentos y registros, incluyendo quién revisa y aprueba los documentos, cómo y dónde se publican, almacenan y protegen?		
25. ¿Es controlada la información documentada de origen externo?		
Operación		
26. ¿La organización tiene la información documentada necesaria para estar segura de que sus procesos se llevan a cabo según lo planeado?		
27. ¿Se controlan los cambios planificados? ¿Las consecuencias de cambios no planificados son revisadas para identificar acciones de mitigación?		
28. ¿Los procesos tercerizados son identificados y controlados?		
29. ¿Los riesgos, sus propietarios, la probabilidad, las consecuencias y el nivel de riesgo son identificados? ¿Estos resultados se encuentran documentados?		
30. ¿Existe un plan de tratamiento del riesgo, aprobado por los propietarios de riesgo?		
31. ¿Hay una lista documentada con todos los controles necesarios, con el estado aplicación y justificación?		
Evaluación del desempeño		
32. ¿Está definido qué tiene que ser medido, a través de qué método, quien es responsable, y quien analizará y evaluará los resultados?		

33. ¿Los resultados de medición son documentados, analizados y evaluados por personas responsables?		

Anexo A. (Continuación)

Análisis de brecha		
Evaluación del desempeño		
34. ¿Existe un programa de auditoría que define las fechas, responsabilidades, reportes, criterios de auditoría y alcance?		
35. ¿Las auditorías internas son realizadas según un programa de auditoría, los resultados se informan a través de un informe de auditoría interna y se levantan o identifican acciones correctivas?		
36. ¿La Revisión por dirección se realizada regularmente, y se documentan los resultados en actas de reunión?		
37. ¿La dirección decide sobre todas las cuestiones cruciales importantes para el éxito del SGSI?		
Mejora		
38. ¿La organización reacciona a cada no conformidad?		
39. ¿La organización considera la eliminación de la causa de la no conformidad, Y en su caso, toma medidas correctivas?		
40. ¿Se registran todas las no conformidades, junto con las acciones correctivas?		
41. ¿El SGSI se ajusta continuamente para mantener su idoneidad, adecuación y eficacia?		

Fuente: Advisera Expert Solutions Ltd. Herramienta gratuita de análisis de brecha para ISO 27001. [En Línea]. 2017. [Citado el 24.Junio.2017]. Disponible en internet: https://advisera.com/27001academy/es/herramientas/herramienta-gratuita-analisis-de-brecha-para-iso-27001/